BANGALORE ELECTRICITY SUPPLY COMPANY LIMITED

OFFICE OF

The General Manager (DAS, SG & TIC),
BESCOM Integrated Control Centre-1,
2nd Sector, 24th Main, 17th Cross,
Opp. BWSSB, HSR Layout,
Bangalore-560102
Mobile: 9448279010

Email: gmdas@bescom.co.in

TENDER DOCUMENT

"Implementation of Cyber - Security Operations Centre (C-SOC) in BESCOM"

Tender Reference: **BESCOM/2025-26/SE0441**

Date and time for commencement of downloading of tender document from the KPP portal *https://kppp.karnataka.gov.in*	As per KPP portal
Last date and time for seeking clarifications if any	As per KPP portal
Date, time and venue of Pre-bid meeting	As per KPP portal
Venue	The General Manager (DAS, SG & TIC), BESCOM Integrated Control Centre-1, 2nd Sector, 24th Main, 17th Cross, Opp. BWSSB, HSR Layout, Bangalore-560102
Last date and time for submission/uploading of tender in the KPP portal *https://kppp.karnataka.gov.in*	As per KPP portal
Date and time for opening of the Technical tenders	As per KPP portal
Date and time for opening of the financial tenders	Will be notified to the qualified tenderers on the KPP portal

KEY EVENTS AND DATES

1	Tender Inviting Authority	GM (DAS,SG&TIC), BESCOM
2	Job Requirement	As per KPP portal (Karnataka Public Procurement Portal https://kppp.karnataka.gov.in)
3	Date of Publication of Tender Document	As per KPP portal
4	Last date of Receiving Queries/ Clarification	As per KPP portal
5	Time, Date and venue of Pre - bid meeting	As per KPP portal
6	Date of Response to Tenderer Queries	As per KPP portal
7	Last Date of Submission of bids	As per KPP portal
8	Bid Processing Fee Payable	As per KPP portal
9	Approximate Estimated value of the tender	As per KPP portal
10	Earnest Money Deposit	As per KPP portal
11	Name of the contact person for any clarification	GM (DAS, SG & TIC), BESCOM Email: gmdas@bescom.co.in Contact No:9448279010
12	Date till which the bid submitted in response to Tender Document is valid	180 days from the last date of submission of bids.

Note: For any doubts regarding uploading documents in KPP Portal (https://kppp.karnataka.gov.in), please contact KPP portal helpline

CONTENTS

Sl. No	SECTION	DESCRIPTION	PAGE NO.
1	Section 1	Invitation for Tenders (IFT)	4-17
2	Section 2	Instructions to Tenderers (ITT)	18-31
4	Section 3	Technical Bid – Standard Forms	32-46
5	Section 4	Financial Bid – Standard Forms	47-48
6	Section 5	Detailed scope of work	49-185
7	Section 6	I Conditions of Contract (CC)	186-194
9		II General Conditions of Contract (GCC)	195-208
10		III Special Conditions of Contract (SCC)	209-215
11	Section 7	Payment Terms and Milestones	216-220
12	Section 8	Appendices	221-230

BANGALORE ELECTRICITY SUPPLY COMPANY LIMITED
(Wholly Owned by Government of Karnataka)

E-mail: gmdas@bescom.co.in

The General Manager (DAS, SG&TIC)
BICC-1,2nd sector, 24th main, 17th cross
HSR Layout, Benagluru-560 102

SECTION-1: INVITATATION FOR TENDERS (IFT)

Invitation for selection of tenderer for "Implementation of Cyber - Security Operations Centre (C-SOC) in BESCOM"

1. The General Manager (Ele.,), DAS, SG&TIC, BESCOM invites tender for "Implementation of Cyber - Security Operations Centre (C-SOC) in BESCOM" from eligible tenderers.
2. More details on the Services to be provided are mentioned in the Detailed Scope of Work of this tender document.
3. The method of selection of tenderer shall be QCBS Method as per the clause 28(C) of KTPP act. The tenderers interested to participate in providing services shall satisfy the following conditions with achieving minimum technical score.

Pre-Qualification Requirements:

Sl.NO	PQ Criteria	Documents to be uploaded by the Bidder
I.	**Technical Pre-Qualification Criteria**	
1.	The Bidder should be in existence as any of the following: a) Company incorporated in India under the Companies Act, 1956/2013 including any amendment thereto;	1. Certificate of Incorporation issued by Registrar of Companies as per Companies Act 1956/2013 along with Memorandum of Association and Articles of Association of the Company. 2. Declaration from Directors of the Company in MBP-1 Form, stating that they are not disqualified to be a Director of the Company, along with the list of Companies in which they

		are Directors as on the date of inviting tender (s).
	b) LLP incorporated in India under the Limited Liability Partnership (LLP) Act, 2008 including any amendment thereto;	1. Certification of Incorporation issued by Registrar of Companies as per LLP Act 2008. 2. Limited Liability Partnership Agreement of LLP.
	c) Partnership Firm under Partnership Act, 1932 in India;	1. Partnership Deed, GST Registration Certificate. 2. Shops & Establishment Registration Certificate, as applicable.
	d) Sole Proprietorship Concern	PAN/GST Registration Certificate
2	a) The Bidder should have the experience of providing and/or implementing at least One On-premises Cyber Security Operations Center (C-SOC) services which includes NG-SIEM, SOAR and UEBA for any State government /Central Government/PSU in India during the last Five Financial Years (2020-21, 2021-22, 2022-23, 2023-24 & 2024-25). b) Cost of any 1 such project said in point (a) shall not be less than 50% (Rs. 15 Crores) of estimated value of contract. Note: Updated to the FY in which the tenders are invited. The value of the completed works shall be given a weightage of 10% per year to bring them to the price level of FY in which the tenders are invited.	a. Work order or Purchase orders b. Completion Certificate signed by an officer of the rank not less than Executive Engineer level or Equivalent.
3	Bidder or his OEM shall be an empanelled cyber security firm by CERT-In.	Valid empanelment certificate issued by CERT-In.

4	The Bidder or his OEM shall have a) ISO 9001:2015 or latest certification. b) ISO 27001:2022 or latest certification	Copies of valid ISO Certificates
II. Financial Requirements		
5	The Annual Turnover of the Bidder in at least Two financial years should not be less than the two times (Rs. 12 Crores.) the estimated annual payments under this contract during the previous Five financial years viz., 2020-21, 2021-22, 2022-23, 2023-24 & 2024-25. Note: Updated to the FY in which the tenders are invited. Financial turnover of previous years shall be given a weight of 10% per year to bring them to the price level of the FY in which the tenders are invited.	Scanned copies of the Audited Annual Accounts statements such as P&L statement, Balance sheets & UDI number of the bidder for the respective FYs shall be uploaded.
6	The Liquid Assets as on 31.01.2026 or at later date before last date of submission of the bid consisting of cash at bank + Term Deposits + availability of fund based credit facilities in any of the Nationalized bank or Scheduled Bank shall not be less than 25% (Rs. 1.5 Crores) of the estimated annual value of contract.	The cash at bank, term deposits and availability of fund based credit facilities shall be supported by a certificate issued by Nationalized/ scheduled Bank shall be uploaded. If the bidder has banking with more than one Bank, then the available liquid assets mentioned above on a particular date i.e., 31.01.2026 or at a later date before submission of bid shall be the same date and time for all the banks.

		In case of Fund based credit facility, the certificate issued by the Nationalized/ Scheduled Bank duly mentioning sanctioned limits, funds utilized so far and balance available as on 31.01.2026 or at a later date, before submission of the bid shall be uploaded.
7	Tender Capacity: The Bidder who meets the above specified minimum qualifying criteria, will only be qualified, if their available tender capacity is more than the Amount Put to tender. The available tender capacity will be calculated as under: Assessed available tender (A*N*1.5-B) capacity A = Maximum value of works executed in any one year during the last five years (updated to FY 2025-26 in which tenders are invited), taking into account the completed as well as works in progress. N = Number of years prescribed for completion of the works for which tenders are invited. B = Value, at FY in which tenders are invited price level, of existing commitments and on-going works to be completed during the next 5 years.	Scanned copy of the statements showing the Total value executed & payment received (excluding GST) in the last five years (FY-2020-21 to FY 2024-25) and UDI number of the bidder duly certified by the Chartered Accountant shall be uploaded. Scanned copy of the statements showing the value of existing commitments & on-going works (Excluding GST) as well as the stipulated period of completion remaining for each of the works as per the format prescribed in the bid documents certified by the Employer in charge, not below the rank of an Executive Engineer or equivalent shall be uploaded. The bidder note that the value of pendency of work (Excluding GST) shall be considered based on financial progress achieved in the particular work as on the date of bid submission.

III.	**General Criteria**	
8	Even though the Bidders meet the above criteria, they are subject to be disqualified if they have: a) Made misleading or false representations in the forms, statements and attachments submitted in proof of the qualification requirements; and/or b) Record of poor performance such as abandoning the services, not properly completing the contract, inordinate delays in completion, litigation history, or financial failures etc.; and/or c) Participated in the previous Tender for the same work and had quoted unreasonably high tender prices and could not furnish rational justification.; and/or d). Black-Listed due to non-performance in execution of works by any central/state govt undertaking utility/ Govt Dept as on date of bid submission. e) Defaulted/short closed due to non-performance in execution of works against the order placed by any central/state govt undertaking electrical utility/ Govt Dept as on date of bid submission.	Scanned copy of Self-Declaration Notarized stamp paper of Rs. 500/- as per the format in the bid document shall be uploaded. Self-declaration shall clearly indicate the tender enquiry number and date on which declaration is done.
9	Any Bidder from a country which shares a land with India will be eligible to bid in this tender only if the bidder is registered with the Competent Authority. (As per Government Order no: FD 455 Exp-12/2020 dt: 25.08.2020). A certificate for having read the clauses is required to be submitted/uploaded by the bidder separately in the following format:	Scanned copy of Self-Declaration Notarized stamp paper of Rs. 500/- as per the format in the bid document shall be uploaded. If the bidder from a country which shares a land with India, Registration certificate issued by the competent authority shall be uploaded.

	I have read the clause regarding restrictions on procurement from a Bidder of a country which shares a land border with India; I certify that this Bidder is not from such a country or, if from such a country, has been registered with the Competent Authority. I hereby certify that this Bidder fulfills all requirements in this regard and is eligible to be considered. (Where applicable, evidence of valid registration by the Competent Authority shall be attached.)	Self-declaration shall clearly indicate the tender enquiry number and date on which declaration is done.
10	The bidder should possess and upload valid Original scanned copy of (a) ESI (b) EPF (c) PAN (d) GST and (e) Registration certificate of Establishment FORM-C (Labour license) issued by the respective competent authorities of the concerned department.	Scanned copy of (a) ESI (b) EPF (c) PAN (d) GST and (e) Registration certificate of Establishment FORM-C (Labour license) issued by the respective competent authorities of the concerned department shall be uploaded.
11	Litigation History: The bidder or his OEMs should provide detailed information on any litigation or arbitration arising out of contracts completed or under execution by it over the preceding five years i.e. FY 2020-21, 2021-22, 2022-23, 2023-24 & 2024-25 A consistent history of awards involving litigation against the bidder may result in rejection of Bid.	Self-declaration on notarized stamp paper of Rs. 500/- shall be uploaded.

Note:

- Bidder shall upload the documents specific to the Qualifying requirement (QR) ONLY. Any general document containing vague information and resemblances to the QR can lead to rejection of the tender.
- The method of selection of firm shall be Quality and Cost Based Selection (QCBS) Method as per the KTPP act.
- Only those bidders who qualify the above pre-qualification criteria will be considered for technical scoring.

Technical Scoring criteria:

The committee decided that the method of selection of firm shall be Quality & Cost Based Selection (QCBS) Method.

Sl No	Minimum eligibility Criteria	Points	Min Points	Max Points
1	**Experience:** The bidder should have the experience of providing and/or implementing at least One On-premises Cyber Security Operations Center (C-SOC) services which includes NG-SIEM, SOAR and UEBA for any State government/Central Government/PSU in India during the last Five Financial Years (2020-21, 2021-22, 2022-23, 2023-24 & 2024-25).	**No of Projects completed** • =1 - 5 Points • >1 - 10 Points	5	10
2	**Financial:** The Annual Turnover of the bidder in at least Two financial years should not be less than the two times (Rs. 12 Crores.) the estimated annual payments under this contract during the previous Five financial years viz., 2020-21, 2021-22, 2022-23, 2023-24 & 2024-25.	**Average Annual Turnover value in Rs. Crores** • 12 crores to 15 crores - 5 Points • > 15 crores - 10 Points	5	10
3	All the proposed solutions (SIEM, SOAR, UEBA, NBAD/NDR) should be deployed for any State government/Central Government/PSU in India during the last Five Financial Years (2020-21, 2021-22, 2022-23, 2023-24 & 2024-	**Deployed in a single Government Organization:** • Less than three out of SIEM, SOAR, UEBA, NBAD– 0 Points • Any three out of SIEM, SOAR, UEBA, NBAD– 6 Points	6	10

	25)., supported with PO/Work order/Invoice copy	• All the proposed solutions (SIEM, SOAR, UEBA, NBAD) – 10 Points		
4	The proposed NBAD/NDR solution should have been successfully implemented for any State government/Central Government/PSU in India during the last Five Financial Years (2020-21, 2021-22, 2022-23, 2023-24 & 2024-25).supported with PO/Work order/Invoice copy	**Number of Employers:** • Less than 1 – 0 Points • 1 to 2 - 7 Points • 2 or more– 10 Points	7	10
5	The bidder should have IT Security professionals on its pay rolls who should be CEH/CISSP/CISA/ CISM/ CCNA/CCNP Certified. Attach supporting documents.	**Number of IT Professionals:** • 10 to 15- 7 Points • 15 or more - 10 Points	7	10
6	The proposed NG-SIEM solution should have been successfully supplied and implemented in an on premise setups in any one Indian Critical Government Organizations with 25000 EPS in the last 5 years considering the capability to support large-scale high-demand environments for future expansions as well, supported with PO/Work order/Invoice copy.	**Supply Experience-Number of references with Events Per Second(EPS):** • No References – 0 Points • = 1 References– 8 Points • >= 2 References–10 Points	15	30
7	Detailed description of the Deliverables, methodology and work plan for performing the Assignment. (Bidders will be asked to	Minimum 0.5 Points and Maximum 2 Points each for the following: 1) Overview of the	5	20

	make a presentation on the above on any day at office of the GM(DAS,SG&TIC), Corporate Office BESCOM) after opening of the Technical bid in KPP Portal.	proposed solution unified NG-SIEM, SOAR, UEBA, NBAD platform in a Single Console(Dashboard) 2) Individual Log Source based Dashboard and Extraction of logs from the Cloud Servers 3) Cyber Kill Chain Dashboard 4) The ability to select data to be visualized from specific data and time range 5) Forensic Analysis for a particular Organization and retrieving 5 Million data within an instant. 6) Flow data collection using custom ports. 7) Showcase of compliance to all the Technical specifications 8) Implementation Plan 9) VAPT Certificate for all the products from CERT-IN empaneled agency 10) IR (Incident Response) Services offered as a part of Contract from OEM		
		Total Points (St1)	**50**	**100**

Proof of Concept Demonstration

Bidder to demonstrate the following features of the proposed tools /solution / platform to the committee appointed by BESCOM

Sl. no.	Criteria	Max points
	NG SIEM	
	Log collection from various log sources: a) Servers & Network devices b) Security devices c) Applications, Active directory etc.	10
	NG SIEM instance support Integration for minimum 25000 EPS per day (Event used for correlation)	10
	Capability for building custom log connectors for non-standard log sources	10
	Creation of use case for threat identification and implementation of correlation rules for threat detection.	10
1	Log parsing capability with advanced AI/ML to detect the incidents for the following minimum set of IT infrastructure security events but not limited to: a. Port & vulnerability scans b. Password cracking c. Worm/virus outbreak d. Unauthorized access to systems e. Intrusion Attempts f. Dos/DDoS Alerts/Attacks	30
	Integration of SIEM with global threat intelligence feeds to collect the threat information a. Commercial threat-intel feeds b. CERT-In threat-intel feeds c. Threat-intel feeds from within OEM's own research labs	20
	Dashboard with management console and role based access to configure the SIEM tool and also to view the details of various incidents	10
2	**NBAD**	

	Ability to monitor and manage different network zones and perform Network Traffic Pattern Analysis based on a. IP addresses b. Groups of IP addresses c. source/destination IP pairs d. Bandwidth Analysis etc	20
	Detect common events like DDoS / DoS, Scanning, Worms, Unexpected application services (e.g., tunneled protocols, backdoors, use of forbidden application Protocols), Policy violations, etc.	10
	Detect Anomalous Security Events and have threshold based alerting.	10
	Get regular feed from global threat intelligence for proactive monitoring and alerting a. Commercial threat-intel feeds b. CERT-In threat-intel feeds b. Threat-intel feeds from within OEM's own research labs	10
3	**UEBA**	
	Ability to highlight risky and potentially abnormal user behavior	20
	Ability to 1. Automatically tweak itself through supervised/unsupervised automated learning 2. Support creation of custom models and or rules/ policy	10
	Dynamically model each device, probabilistically identifying any anomalous activity that falls outside of the device's normal pattern of life	10
4	**SOAR**	
	Ability to design automation playbooks	10
	Ability to integrate with NG-SIEM, NBAD, UEBA etc.	10
	Ability to integrate with security devices like firewall, Anti-virus, IPS, IDS etc. for automating the configuration of security rules	10
5	**Threat Intelligent Platform**	

	In-built Machine Learning based searches to perform threat hunting on 24x7 basis/real time	10
	Ability to store queries and execute queries on a periodic basis/as per Employer requirement	10
6	**External Attack Surface Monitoring**	
	Ability to detect, monitor and shutdown all kinds of incidents given below: Phishing, Pharming, Brand Abuse, rouge websites and mobile apps related to BESCOM, Email address used for fraudulent purpose.	10
	Detection Mechanisms to track usage of BESCOM digital watermark, Real-time monitoring of web-server referrer logs. Track new domain name registrations to detect any spoofed site being registered. Monitor & report abuse mailbox provided to customers	10
7	**Deception solution**	
	Using dynamically refreshed deceptive objects and projection of high interaction traps (decoys) in the network to lure the attackers.	10
	Securing Active Directory from AD reconnaissance activities from endpoints.	2
	Inbuilt sandbox to perform malware analysis and provide detailed forensics and TTP (Tactics, Techniques and Procedures) of the attacker/malware.	2
	Dedicated sinkhole port capability to provide a safe line for internet for attacker on a trap (decoy).	2
	Coverage of deception at branch and remote offices and detecting layer 2 attacks like MiTM at branch/remote offices.	4
8	**Ticketing Tool**	
	The Bidder shall have implemented the proposed ITSM solution in at least one Government / PSU / utility organization during the last 05 years.	10
	The ITSM tool shall support native or API-based integration with SIEM, SOAR, Active Directory/LDAP, email, and monitoring tools for automated ticket creation and updates.	2

	The ITSM tool shall provide configurable SLA policies, priority-based escalation matrix, breach alerts, and auto-notifications to stakeholders.	2
	The ITSM solution shall support role-based access control (RBAC), multi-factor authentication, audit logs, and data encryption at rest and in transit.	2
	The ITSM solution shall be available in on-prem / private cloud / government cloud deployment models and be scalable to support multi-location operations and 24x7 services.	2
	The ITSM tool shall provide configurable SLA policies, priority-based escalation matrix, breach alerts, and auto-notifications to stakeholders.	2
Total		**300**
St2		**St2 = Total / 3**
Grand Total		**St = (St1 + St2) /2**

Note: The bidders to note that the above-mentioned marks in St1=100 points and St2=100 points. [St=(St1+St2)/2] will be apportioned to 100 points in KPP portal.

The minimum technical score required to qualify is 70 Points. Each responsive proposal will be given a technical score (St). A proposal shall be rejected at this stage if it fails to achieve the minimum technical score of 70 points.

The lowest Financial Bid (Fm) will be given a financial score (Sf) of 100 points. The financial scores (Sf) of the other Financial Bids will be computed as below: Sf = 100 x Fm/F, in which Sf is the financial score, Fm is the lowest price, and F the price of the proposal under consideration.

Bids will be ranked according to their combined technical (St) and financial (Sf) scores using the weights (T = the weight given to the Technical Bid; P = the weight given to the Financial Bid; T + P = 1) indicated in the Data Sheet: S=St * T% + Sf * P%. The tenderer achieving the highest combined technical/ financial score will be invited for negotiations and further process for awarding the contract (T=0.70 and P=0.30).

4. Even though the tenderers meet the above criteria, they are subject to be disqualified if they have:
   - made misleading or false representations in the forms, statements and attachments submitted in proof of the qualification requirements; and/or

- record of poor performance such as abandoning the works, not properly completing the contract, inordinate delays in completion, litigation history, or financial failures etc.

5. Interested tenderers may submit their proposals for implementation of the proposed work along with requisite EMD declaration (as notified in the KPP Portal) through online at https://www.kppp.karnataka.gov.in.

6. **Earnest money deposit:** Please refer EMD clause (clause 13 as per ITT)

7. Tender Processing fee: As per stipulation in the KPP portal

8. Price Schedule (For Information to tenderers):

Components	**Estimated Cost inclusive of GST (in Crores.)**
One time setup cost along with licensing charges for all the tools mentioned in BOQ for 6 months period implementation phase	3.68
Annual maintenance that includes all technical subscription charges for 5 years	16.12
Human Resource Cost in crores for 5 years	9.94
Total project cost for 5 years 6 months	**29.74**

Note: The tenderer needs to quote in lump sum against the total project cost for 5 years 6 months.

The price breakup for the individual items based on the Payment Schedule (as per Table 2 of clause 2 in SECTION 7: Payment Terms and Milestones – C-SOC Implementation) will be obtained as per the Clause 10.2 of ITT from the successful tenderer.

SECTION 2: INSTRUCTION TO TENDERERS (ITT)

A: General

1.Scope of Tender:

The Bangalore Electricity Supply Company Limited invites tender for **Implementation of Cyber - Security Operations Centre (C-SOC) in BESCOM.**

C-SOC (Cyber Security Operations Centre) architecture shall provide centralized cybersecurity monitoring for IT, OT, and IoT Systems, Web and Mobile Applications of BESCOM through a layered, DMZ-based design ensuring strict IT-OT segregation. The SOC shall utilize SIEM, SOAR, UEBA, and NBAD platforms and other tools with controlled, secure, and encrypted data flow from field and operational systems, ensuring compliance with CEA and CERT-In guidelines while maintaining operational safety of power distribution systems conforming to technical specifications stipulated in the tender.

2.Eligible Tenderers:

2.1 Tenderers shall not be under a declaration of ineligibility for corrupt and fraudulent practices issued by the Government of Karnataka.
2.2 Tenders from Joint ventures are not acceptable.

3.Qualification of the Tenderer: Please refer Clause 3, Section 1 of IFT

4. VOID.

5. Cost of Tendering:

The tenderer shall bear all costs associated with the preparation and submission of his tender, and the Employer will in no case be responsible and liable for those costs.

6. Site visit:

The Tenderer at his own responsibility and risk is encouraged to visit and examine the Site of Works and its surroundings and obtain all information that may be necessary for preparing the Tender and entering into a contract for construction of the Works. The cost of visiting the Site shall be at the Tenderer's own expense.

B. Tender documents

7. Content of Tender Documents

7.1 The set of tender documents shall have all the Sections given in Contents
7.2 Both the sets should be completed and returned with the tender.

8.Clarification of Tender Documents: (Pre Bid Meeting)

8.1 A prospective tenderer requiring any clarification of the tender documents may notify the Employer in writing or by mail or to the Employer's address indicated in the invitation to tender. The Employer will respond to any request for clarification which he receives earlier than 15 days prior to the deadline for submission of tenders. Clarifications for the same shall be uploaded in KPP portal.

8.2 **Pre-Bid meeting:**

8.2.1 The tenderer or his authorized representative is invited to attend a pre-tender meeting which will take place as per calendar uploaded in the KPP Portal.

8.2.2 VOID

8.2.3 The tenderer is requested to submit any questions in writing or by email to reach the Employer on or before the Pre bid meeting.

8.2.4 VOID

8.2.5 Non-attendance at the pre-bid meeting will not be a cause for disqualification of a tenderer.

9. **Amendment of Tender documents**

9.1 Before the deadline for submission of tenders, the Employer may modify the tender documents by issuing addenda.

9.2 Any addendum thus issued shall be part of the tender documents shall be uploaded in the KPP portal.

9.3 To give prospective Tenderers reasonable time in which to take an addendum into account in preparing their tenders, the Employer shall extend as necessary the deadline for submission of tenders, in accordance with Sub-Clause 16.2 below.

C. Preparation of Tenders

10. **Documents comprising the Tender**

10.1 The tender submitted by the Tenderer shall be in two-part system as per KPP Portal and shall contain the documents as follows:

10.1.1 First part- technical bid as per KPP portal

a. Earnest Money Deposit;
b. Qualification Information as per formats given as per PQ Requirement as detailed in clause 3.

- In preparing the Technical Bid, tenderers are expected to examine the documents comprising this tender documents in detail. Material deficiencies in providing the information requested may result in rejection of a Bid.

- While preparing the Technical Bid, tenderers must give particular attention to the following:

- For assignments on a staff-time basis, the estimated number of key professional staff-months is given in the Data Sheet. The bid shall, however, be based on the number of key professional staff-months estimated by the firm.

- It is desirable that the majority of the key professional staff proposed be permanent employees of the firm or have an extended and stable working relation with it.

- Proposed key professional staff must at a minimum have the experience indicated in the Data Sheet.

- Alternative key professional staff shall not be proposed, and only one curriculum vitae (CV) may be submitted for each position.

- Reports to be issued by the tenderers as part of this assignment must be in the language(s) specified in the Data Sheet. It is desirable that the firm's personnel have a working knowledge of the Employer's official language.

- The Technical Bid should provide the following information using the attached Standard Forms (Section 3)

- A brief description of the tenderer's organization and an outline of recent experience on assignments (Section 3B) of a similar nature. For each

assignment, the outline should indicate, inter alia, the profiles and names of the staff provided, duration of the assignment, contract amount, and firm's involvement.

- Any comments or suggestions on the Detailed scope of work and on the data, a list of services, and facilities to be provided by the Employer (Section 3C).

- A description of the methodology and work plan for performing the assignment (Section 3D).

- The list of the proposed staff team by specialty, the tasks that would be assigned to each staff team member, and their timing (Section 3E).

- CVs recently signed by the proposed key professional staff and the authorized representative submitting the bid (Section 3F). Key information should include number of years working for the firm/entity, and degree of responsibility held in various assignments during the last ten (10) years.

- A detailed description of the proposed methodology, staffing, and monitoring of training, if the Data Sheet specifies training as a major component of the assignment.

- Any additional information requested in the Data Sheet.

- The Technical Bid shall not include any financial information.

10.1.2 Second part: - Price bid (Financial bid) as per KPP Portal

(a) The Tender (in the format indicated in Section 4)
(b) Priced Bill of Quantities.
and any other materials required to be completed and submitted by Tenderers in accordance with these instructions. The documents listed under Sections 3, 4, 6 and 9 shall be filled in without exception.

10.2 In preparing the Financial Bid, tenderers are expected to take into account the requirements and conditions of the bidding documents. The Financial Bid should follow Standard Forms (Section 4).

- The tenderers should quote their total price offer in lump sum in KPP portal for all the services sought by BESCOM in the detailed scope of work of this tender document, including all applicable Taxes. The breakup of cost for all items of the Tender documents shall be provided to the employer in the event

of the order. Tenderers shall express the price of their services in Indian Rupees.

- The Data Sheet indicates how long the bids must remain valid after the submission date. During this period, the tenderer is expected to keep available the key professional staff proposed for the assignment. The Employer will make its best effort to complete negotiations within this period. If the Employer wishes to extend the validity period of the bids, the tenderers who do not agree have the right not to extend the validity of their bids.

11 Tender prices:

11.1 The contract shall be for the whole works as described in Clause 1 based on the priced Bill of Quantities submitted by the Tenderer.

11.2 The Tenderer shall fill in rates and prices (both in figures and words) for all items of the Works described in the Bill of Quantities along with total tender price (both in figures and words). Items for which no rate or price is entered by the Tenderer will not be paid for by the Employer when executed and shall be deemed covered by the other rates and prices in the Bill of Quantities. Corrections, if any, shall be made by crossing out, initialing, dating and rewriting. The Tenderer should quote their total price offer in KPP portal for all the services sought by the BESCOM in the Detailed scope of work, including all applicable Taxes. The breakup of cost for all items of the tender shall be provided to the employer in the event of the order firm shall express the price of their services in Indian Rupees.

11.3 All duties, taxes, and other levies payable by the contractor under the contract, or for any other cause, shall be included in the rates, prices and total Tender Price submitted by the Tenderer.

11.4 VOID

12 Tender validity

12.1 Tenders shall remain valid for a period 180 days after the deadline date for tender submission specified in Clause 16

12.2 In exceptional circumstances, prior to expiry of the original time limit, the Employer may request that the Tenderers may extend the period of validity for a specified additional period. The request and the Tenderers' responses shall be made in writing or by mail. A Tenderer may refuse the request without forfeiting his earnest money deposit. A Tenderer agreeing to the request will not be required or permitted to modify his tender, but will be required to extend the validity of his earnest money deposit for a period of the extension, and in

compliance with Clause 13 in all respects.

13.Earnest money deposit

13.1 Earnest Money Deposit- (EMD)

13.2 The tenderers are requested to pay EMD as indicated in the KPP portal along with the Technical Bid.

13.3 The tenderer can pay the Earnest Money Deposit (EMD) in the KPP portal.

13.4 The tenderer's bid will be evaluated only on confirmation of receipt of the payment (EMD) in the Government of Karnataka central pooling account held at designated Bank. EMD amount will have to be submitted by the tenderer taking into account the following conditions:

a. EMD will be accepted only in the form of electronic cash (and not through Demand Draft or Bank Guarantee) and will be maintained in the Government's central pooling account at designated Bank until the contract is closed.
b. The entire EMD amount for a particular tender has to be paid in a single transaction. It is responsibility of tenderer to ensure that payment through NEFT reaches Payment to Government of Karnataka's designated Bank Before Bid submission date and time, through online payment.

For the details on e-Payment services refer to KPP portal for more details on the process.

13.5 REFUND OF EMD

Based on the instructions of Tender Accepting Authority (TAA) the EMD amount of the unsuccessful tenderers will be refunded to the respective Bank accounts of the tenderer registered in the KPP PORTAL.

- The earnest money deposit of unsuccessful tenderer will be returned after the award of proposal to the successful tenderer.

- The earnest money deposit of the successful tenderer will be discharged when the tenderer has furnished the required Performance Security and signed the Agreement.

- The earnest money deposit may be forfeited:

i. if the tenderer withdraws the proposal after deadline for submission of proposals, during the period of proposal validity;
ii. in the case of a successful tenderer, if the tenderer fails within the specified time limit to furnish the required Security deposit or sign the Agreement.
iii. in case of tenderer submitting fake documents such as Annual financial turn over, work done certificate etc., relevant to the proposal.

The original Bid (Technical Bid and Financial Bid; shall be as per clause per clause 10.1 of the ITT

14. Format and signing of Tender

14.1 An authorized representative of the tenderer shall digitally sign the Bid in KPP portal. The representative's authorization is confirmed by a written power of attorney accompanying the Bid.

14.2 The tenderer shall submit the bids separately i.e., **Technical and Financial** electronically online in Government of Karnataka KPP portal.

14.3 Tenderer has all the time to modify and correct or upload any relevant document in the portal before submission on KPP portal. The last date and time including hours, minutes and seconds for submission will be mentioned in the portal, the bid will disappear automatically immediately after the time of submission is elapsed. After the deadline for submission of bids, the Technical Bid shall be opened by the evaluation committee and evaluation will be done. The tenderers who are technically qualified will be intimated through KPP portal only.

D. Submission of Tenders

15. VOID

16. **Deadline for submission of the Tenders** as per Calendar of events: As per KPP Portal calendar of events.

16.1 Tenders must be received by the Employer at the address specified above no later than. As per KPP portal deadline In the event of the specified date for the submission of tenders being declared a holiday for the Employer, the tenders will be received up to the appointed time on the next working day.

16.2 The Employer may extend the deadline for submission of tenders by issuing an amendment in accordance with Clause 9, in which case all rights and obligations of the Employer and the Tenderers previously subject to the original deadline will then be subject to the new deadline.

17. VOID

18. **Modification and Withdrawal of Tenders:** No modifications of the tenders or withdrawal of tenders.

E. Tender opening and evaluation

19. Opening of Technical Bid of all Tenders and evaluation to determine qualified Tenderers:

BID EVALUATION

- From the time of bids are opened to the time the contract is awarded, if any tenderer wishes to contact the Employer on any matter related to its bid, it should do so in writing at the address indicated in the Data Sheet. Any effort by the firm to influence the Employer in the Employer's bid evaluation, bid comparison or contract award decisions may result in the rejection of the tenderer's bid.

- Evaluators of Technical Bids shall have no access to the Financial Bids until the technical evaluation, including its approval by competent authority is obtained.

Evaluation of Technical Bids

- The technical bids are evaluated as per KTPP on the following basis:
  - Payment of EMD
  - Eligibility criteria specified (PQR) and the documents furnished by the Tenderer in technical bid in support of meeting the eligibility criteria and the score obtained under QCBS method
  - Presentation/demonstration on the technical specifications and functionalities and the score obtained under QCBS method
- The technical bids shall not contain the financial part of the bid. In case the prices are disclosed at technical evaluation stage, the bid is liable for rejection as a whole.

- Verification of original documents: The tender inviting authority reserve the right to verify the original documents, copies of which submitted through KPP Portal during the submission of tender. The tenderer shall produce the Original Documents during the Demonstration of the Application/Software or as and when requested by the Tender inviting authority. Failure on the part of the Tenderer to produce original document on demand at any point of time may result in rejection of the bid.
- Submission of Original Documents: It is mandatory that, the Successful tenderer shall submit following documents in original with original seal and signature (of which the softcopies uploaded through KPP portal) within 7 days, from last date prescribed for submission of Technical Bids, such as Forms of Annexure Forms of Specification/technical compliance, Affidavits/Declarations specific for the tender, Documents/communications particularly addressed to Tender inviting authority/or limited to Current tender.
- The Employer may waive any minor informality or non-conformity or irregularity in a supporting document being submitted against meeting the eligibility criteria, which does not constitute a material deviation from the eligibility criteria and technical/specification requirement prescribed, provided such a waiver does not prejudice or affect the relative ranking of any Tenderer. For this provision, the Tender Inviting authority or the Tender Accepting authority or the Tender Scrutiny Committee may seek bonafide clarifications from Tenderers during the evaluation of tenders under Rule 23(3) of Karnataka Transparency in public Procurement Rules. 2000.
- The bids are evaluated strictly against the terms and conditions of the tender as a whole and any counter offer or conditional offer with regard to delivery period, payment, specification, scope of the work etc., will be ignored and deemed to be invalid unless it is specifically noted and accepted by the competent authority during the evaluation/acceptance of the bids. No claim of the tenderer will be considered in such instances at later stage.

Note: Tenderer shall upload the documents specific to the Qualifying requirement (QR) ONLY. Any general document containing vague information and resemblances to the QR can lead to rejection of the tender.

- The evaluation committee appointed by the Employer as a whole, and each of its members individually, evaluates the bids on the basis of their responsiveness to the Detail scope of work, applying the evaluation criteria and point system specified in the Data Sheet.

The tenderers qualifying the above Pre-Qualification criteria will be evaluated as per the point system specified for technical evaluation criteria in the data sheet based on the documents uploaded and technical demonstration by the tenderer to the committee appointed by BESCOM.

As per KTPP Act 28C,

The quality and cost based selection is based both on the quality of the proposals and the cost of the services to be provided. In this method, the technical and financial proposals shall be received in separate sealed envelope. The technical proposals shall be opened first (unopened financial proposals are kept under security) and the evaluation report of the technical proposals shall be prepared and the approval of Tender Accepting Authority shall be obtained. The financial envelopes of those consultants who submitted responsive technical proposals meeting the minimum qualifying scores shall be opened in the presence of the consultants or their representatives. The proposals shall then be evaluated. Once the financial proposals are evaluated, a combined evaluation of the technical and financial proposals shall be carried out by weighing and adding the quality and the cost scores, and the Consultant obtaining the highest combined score shall be invited for negotiations. Since price is a factor of selection, staff rates and other unit rates shall not be negotiated.

Each responsive bid will be given a technical score (St). A bid shall be rejected at this stage if it does not respond to important aspects of the Detail scope of work or if it fails to achieve the minimum technical score indicated in the Data Sheet.

The Employer shall prepare minutes of the Tender opening, as procedure stipulated in the KPP Portal.

20. Evaluation of Financial Bids:

- After the evaluation is completed, the Employer shall notify those tenderers whose bids did not meet the minimum qualifying mark or were considered non-responsive to the tender document in the KPP portal only. The Employer shall simultaneously notify the tenderers that have secured the minimum qualifying mark, indicating the date and time set for opening the Financial Bids. The date of opening of financial bid will be notified in KPP portal only.

- The lowest Financial Bid (Fm) will be given a financial score (Sf) of 100 points. The financial scores (Sf) of the other Financial Bids will be computed as indicated in the Data Sheet. Bids will be ranked according to their combined technical (St) and financial (Sf) scores using the weights (T = the weight given to the Technical Bid; P = the weight given to the Financial Bid; T + P = 1) indicated in the Data Sheet: S=St * T% + Sf * P%. The tenderer achieving the highest combined technical/ financial score will be invited for negotiations and further process for awarding the contract.

21. Process to be confidential

21.1 Information relating to the examination, clarification, evaluation, and comparison of Tenders and recommendations for the award of a contract shall not be disclosed to Tenderers or any other persons not officially concerned with such process until the award to the successful Tenderer has been announced. Any effort by a Tenderer to influence the Employer's processing of Tenders or award decisions may result in the rejection of his Tender.

22 Clarification of Tenders:

22.1 To assist in the examination, evaluation, and comparison of Tenders, the Employer may, at his discretion, ask any Tenderer for clarification of his Tender, including breakdowns of unit rates. The request for clarification and the response shall be in writing or by email, but no change in the price or substance of the Tender shall be sought, offered, or permitted except as required to confirm the correction of arithmetic errors discovered by the Employer in the evaluation of the Tenders in accordance with Clause 24.

22.2 Subject to sub-clause 22.1, no Tenderer shall contact the Employer on any matter relating to its Tender from the time of the Tender opening to the time the contract is awarded. If the Tenderer wishes to bring additional information to the notice of the Employer, it should do so in writing.

22.3 Any effort by the Tenderer to influence the Employer in the Employer's Tender evaluation, Tender comparison or contract award decisions may result in the rejection of the Tenderers' Tender.

23. Examination of Tenders and determination of responsiveness:

23.1 Prior to the detailed evaluation of Tenders, the Employer will determine whether Tender;
(a) has been properly signed; as per KPP Portal
(b) is substantially responsive to the requirements of the Tender documents.

23.2 A substantially responsive Tender is one which conforms to all the terms, conditions, and specifications of the Tender documents, without material deviation or reservation. A material deviation or reservation is one (a) which affects in any substantial way the scope, quality, or performance of the Works; (b) which limits in any substantial way, inconsistent with the Tender documents, the Employer's rights or the Tenderer's obligations under the

Contract; or (c) whose rectification would affect unfairly the competitive position of other Tenderers presenting substantially responsive Tenders.

23.3 If a Tender is not substantially responsive, it will be rejected by the Employer, and may not subsequently be made responsive by correction or withdrawal of the nonconforming deviation or reservation.

24. VOID

25. **Evaluation and comparison of Tenders:**

25.1 The Employer will evaluate and compare only the Tenders determined to be substantially responsive in accordance with Clause 23.

25.2 VOID

25.3 VOID

25.4 VOID

25.5 VOID

F. Award of Contract

26. **Award criteria**

26.1 Subject to Clause 27, the Employer will award the Contract to the Tenderer whose Tender has been determined to be substantially responsive to the Tender documents and who has offered the lowest evaluated Tender Price, provided that such Tenderer has been determined to be
(a) eligible in accordance with the provisions of Clause 2, and
(b) qualified in accordance with the provisions of Clause 3.

27. **Employer's right to accept any Tender and to reject any or all Tenders**

27.1 Notwithstanding Clause 26, the Employer reserves the right to accept or reject any Tender, and to cancel the Tender process and reject all Tenders, at any time prior to the award of Contract, without thereby incurring any liability to the affected Tenderer or Tenderers or any obligation to inform the affected Tenderer or Tenderers of the grounds for the Employer's action.

28. **Notification of award and signing of Agreement**

28.1 The Tenderer whose Tender has been accepted will be notified of the award by the Employer prior to expiration of the Tender validity period by email

confirmed by registered/speed post issuing letter of Intent. This letter (hereinafter and in the Conditions of Contract called the "Letter of Acceptance") will state the sum that the Employer will pay the Contractor in consideration of the execution, completion, and maintenance of the Works by the Contractor as prescribed by the Contract (hereinafter and in the Contract called the "Contract Price").

28.2 The notification of award will constitute the formation of the Contract, subject only to the furnishing of Security deposit in accordance with the provisions of Clause 29.

28.3 The Agreement will incorporate all agreements between the Employer and the successful Tenderer. It will be kept ready for signature of the successful Tenderer in the office of Employer within 30 days following the notification of award along with the Letter of Acceptance. Within 20 days of receipt, the successful Tenderer will sign the Agreement and deliver it to the Employer.

28.4 Upon the furnishing by the successful Tenderer of the Performance Security, the Employer will promptly notify the other Tenderers that their Tenders have been unsuccessful.

29. Security deposit:

29.1 Within 15 days of receipt of the Letter of Acceptance, the successful Tenderer shall deliver to the Employer a Security deposit in any of the forms given below for an amount equivalent to 5% of the Contract price plus additional security for unbalanced tenders in accordance with Clause 25.5 of ITT and Clause 44 of the Conditions of Contract:
- bank guarantee / e-bank guarantee in the form given in Section 10;

29.2 If the security deposit is provided by the successful Tenderer in the form of a Bank Guarantee, it shall be issued either by a Nationalized Banks/ Scheduled Commercial Banks approved by Reserve Bank of India.

29.3 VOID

29.4 Failure of the successful Tenderer to comply with the requirements of Sub-Clause 29.1 shall constitute sufficient grounds for cancellation of the award and forfeiture of the Earnest money deposit.

PERFORMANCE SECURITY

- Within 15 days of issue of the Letter of Intent in KPP portal (a copy will be submitted through e-mail as well), the successful tenderer shall deliver to the Employer a Security deposit in the form of Bank Guarantee in the favor of

BESCOM at an amount equivalent to 5% (Five percent) of the Contract price.

- Performance Security shall be provided to the Employer not later than the date specified in the Letter of Intent and shall be issued in an amount and form and type of instrument acceptable to the Employer. The Security deposit shall remain valid for a period of 60 days from the date of expiry of contract period.

- The Performance Security shall be furnished from any Nationalized Banks/ Scheduled Commercial Banks approved by Reserve Bank of India.

- Prior to including a claim under the performance Guarantee the Employer shall in every case notify the contractor stating the nature of the default in respect of which the claim is made.

30. VOID

31. Corrupt or Fraudulent practices:

31.1 The GOK requires that the Tenderers/Suppliers/Contractors, observe the highest standard of ethics during the procurement and execution of such contracts. In pursuance of this policy, GOK:

(a) will reject a proposal for award if it determines that the Tenderer recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question;

(b) will declare a firm ineligible, either indefinitely or for a stated period of time, to be awarded a GOK contract if it at any time determines that the firm has engaged in corrupt or fraudulent practices in competing for, or in executing, a GOK contract.

31.2 Furthermore, Tenderers shall be aware of the provision stated in sub-clause 50.2 of the Conditions of Contract.

SECTION 3. TECHNICAL BID - STANDARD FORMS
(To be filled out and uploaded in the KPP portal)

3A. Technical Bid submission form.

3B. Tenderer's references

3C. Comments and suggestions on the Detailed scope of work and on data services, and facilities to be provided by the Employer.

3D. Description of the methodology and work plan for performing the assignment.

3E. Team composition of task assignments.

3F. Format of Curriculum Vitae of proposed key professional staff.

3G. Power of Attorney of Authorized Signatory

3H. Summary of the CV's of Key Staff Proposed

3I. Summary of tenderer Annual Turnover.

3J: Summary of tenderer Experience/Qualifications.

3K. Affidavit regarding correctness of information furnished and documents submitted.

3L. Technical compliance of the tools/platform proposed for assessment.

3M. Form for Bid Capacity.

3A. TECHNICAL BID SUBMISSION FORM
(On the letter Head of the Tenderer)

[*Location, Date*]

FROM: (Name of Tenderer)

To,
The General Manager (Ele),
DAS, SG & TIC
Corporate office, BESCOM
Bangalore.

Sir,

Subject: **"Implementation of Cyber – Security Operations Centre (C-SOC) in BESCOM"– Regarding Technical Bid.**

We, the under signed, offer to provide the services for the above in accordance with your Request for Proposal notified in the KPP portal as Enquiry No: BESCOM/2025-26/SE0441**.** We are hereby submitting our Bid which includes this Technical Bid, and a Financial Bid encrypted in Government of Karnataka KPP portal.

We hereby declare that all the information and statements made in this Bid are true and accept that any misinterpretation contained in it may lead to our disqualification.

If negotiations are held by the EMPLOYER, we undertake to attend negotiations. Our Bid is binding upon us and subject to the modifications resulting from contract negotiations, up to expiry of the validity period of the bid.

We understand you are not bound to accept any Bid you receive.

We remain,

Yours sincerely,

Authorized Signature [In full and initials]: _____

Name and Title of Signatory: _____
Name of Tenderer:_____
Address: _____

3B. TENDERER'S REFERENCES

Tenderer's Organization

[Provide here a brief (two pages) description of the background and organization of your firm/ entity and each associate for this assignment.]

Tenderer's Experience
Relevant Services Carried Out in the Last Five Years
That Best Illustrate Qualifications

[Using the format below, provide information on each assignment for which your firm for this assignment, was legally contracted for carrying out services similar to the ones requested under this assignment.]

Assignment name:	Value of works for which services is obtained: (Indian Rs): Value of the contract: (Indian Rs):
Country: Location within country:	Duration of assignment (months):
Name of Employer:	Key professional staff Provided by Your Firm/entity(profiles):
Address:	Number of Staff assigned for the project:
Start date (month/year): Completion date (month/year):	Name of senior professional staff of your firm involved and functions performed (indicate most significant profiles such as Project Director/Coordinator, Team Leader):
Narrative description of Project:	
Description of actual services provided by your staff within the assignment:	

Authorized Signature [In full and initials]: _____
Name and Title of Signatory: _____
Name of Tenderer: _____
Address: _____

Note: Along with this format, the Experience certificate from the officer not below the rank of Executive Engineer or equivalent of the concerned utility shall be attached.

3C. COMMENTS AND SUGGESTIONS OF TENDERER ON DETAILED SCOPE OF WORK AND ON DATA, SERVICES, AND FACILITIES TO BE PROVIDED BY THE EMPLOYER

On the Detailed Scope of Work:

1.

2.

3.

4.

5.

On the data, services, and facilities to be provided by the Employer

1.

2.

3.

4.

5.

3D. DESCRIPTION OF THE METHODOLOGY AND WORK PLAN FOR PERFORMING THE ASSIGNMENT

TENDERER'S NAME:

Technical approach, methodology and work plan are key components of the Technical Bid. You are suggested to present your Technical Bid divided into the following three chapters:

a) Technical Approach and Methodology,
b) Work Plan, and
c) Organization and Staffing,

a. *Technical Approach and Methodology: In this chapter the tenderer should explain their understanding of the objectives of the Assignment/job, approach to the Assignment/job, methodology for carrying out the activities and obtaining the expected output, and the degree of detail of such output. Agency should highlight the problems being addressed and their importance, and explain the technical approach the agency would adopt to address them. Agency should also explain the methodologies they propose to adopt and highlight the compatibility of those methodologies with the proposed approach.*

b. *Work Plan: The tenderer should propose and justify the main activities of the Assignment/job, their content and duration, phasing and interrelations, milestones (including interim approvals by the EMPLOYER), and delivery dates of the reports. The proposed work plan should be consistent with the technical approach and methodology, showing understanding of the Detailed Scope of Work and ability to translate them into a feasible working plan. A list of the final documents, including reports, drawings, and tables to be delivered as final output, should be included here. The work plan should be consistent with the Work Schedule.*

c. *Organization and Staffing .In this chapter tenderer should propose the structure and composition of team. Tenderer should list the main disciplines of the assignment, the key expert responsible, and proposed technical and support staff.*

3E. TEAM COMPOSITION AND TASK ASSIGNMENTS

1. **Key Staff : [L1/L2/L3/L1 Consultant GRC (Governance, risk management, and compliance) Team/L2 Consultant GRC (Governance, risk management, and compliance)Team/ L1 Engineer Tools Management/L2 Engineer Tools Management/L2 Engineer Application and Network Security]**

Name of Staff	Qualification	Year of Experience	Position Assigned	Task Assigned

2. Support Staff

Name of Staff	Qualification	Year of Experience	Position Assigned	Task Assigned

Authorized Signature [In full and initials]: _____

Name and Title of Signatory: _____

Name of Tenderer: _____

Address: _____

3F. FORMAT OF CURRICULUM VITAE (CV) FOR PROPOSED KEY PROFESSIONAL STAFF

Proposed Position:

Name of Tenderer:

Name of Staff:

Profession:

Date of Birth:

Years with Firm/Entity: _____Nationality:

Membership in Professional Societies:

Detailed Tasks Assigned:
[List all tasks to be performed under this assignment]

Key Qualifications:
[*Give an outline of staff member's experience and training most pertinent to tasks on assignment. Describe degree of responsibility held by staff member on relevant previous assignments and give dates and locations.*]

Education:
[*Summarize college/university and other specialization of staff member, giving names of schools, dates attended, and degrees obtained.*]

Employment Record:

[*Starting with present position, list in reverse order every employment held. List all positions held by staff member since graduation, giving dates, names of employing organizations, titles of positions held, and locations of assignments. For experience in the years mentioned in RFP, also give types of activities performed and Employer references, where appropriate.*] (copy of Experience certificate shall be attached)

Languages:
[*For each language indicate proficiency: excellent, good, fair, or poor; in speaking, reading, and writing]*

Certification:

I, the undersigned, certify that to the best of my knowledge and belief, these data correctly describe me, my qualifications, and my experience.

I, the undersigned further certify that I am willing to carry out this assignment and I confirm my availability to this assignment, if assignment is awarded to our firm.

I understand that any willful misstatement described herein may lead to my disqualification or dismissal, if engaged.

Full name of the Tenderer and Signature of Authorized Signatory

Date:
Place:

3G. Power of Attorney of Authorized Signatory

(To be executed on appropriate non judicial stamp paper)

We…… (name of the firm and address of the registered office) do hereby irrevocably constitute, nominate, appoint and authorise Mr/ Ms (name), …… son/daughter/wife of …… and presently residing at ……, who is presently employed with us and holding the position of …… , as our true and lawful attorney (hereinafter referred to as the "Authorized Signatory") to do in our name and on our behalf, all such acts, deeds and things as are necessary or required in connection with or incidental to submission of our application for pre-qualification and submission of our bid by the General Manager (Ele), (DAS,SG&TIC), Corporate office, BESCOM (the "General Manager (Ele), DAS,SG&TIC, BESCOM herein after refer to as the EMPLOYER") including but not limited to signing and submission of all applications, bids and other documents and writings, participate in Pre-Bid Conference and other meetings and providing information/ responses to the EMPLOYER, representing us in all matters before the EMPLOYER, signing and execution of all contracts and undertakings consequent to acceptance of our bid, and generally dealing with the EMPLOYER in all matters in connection with or relating to or arising out of our bid for the said Assignment and/ or upon award thereof to us.

AND we hereby agree to ratify and confirm all acts, deeds and things done or caused to be done by our said Attorney pursuant to and in exercise of the powers conferred by this Power of Attorney and that all acts, deeds and things done by our said Authorized Signatory in exercise of the powers hereby conferred shall and shall always be deemed to have been done by us.

IN WITNESS WHEREOF WE, ……, THE ABOVE NAMED IN PRINCIPAL HAVE EXECUTED THIS POWER OF ATTORNEY ON THIS …… DAY OF ……, 2020

For

……

(Signature, name, designation and address)

Witnesses:

1.

2. (Notarised)

Accepted

……

(Signature)

(Name, Title and Address of the Authorized Signatory)

Note:

1. The mode of execution of the Power of Attorney should be in accordance with the procedure, if any, laid down by the applicable law and the charter

documents of the executants(s) and when it is so required the same be affixed under common seal in accordance with the required procedure. The Power of Attorney should be on a stamp paper of appropriate value.

2. Also, wherever required, the Tenderer should submit for verification the extract of the charter documents such as a resolution/power of attorney in favour of the Person executing this Power of Attorney for the delegation of power hereunder on behalf of the Tenderer.

3 H. SUMMARY OF THE CV's OF KEY STAFF PROPOSED:

Sl. No	Key Professionals	Required Nos.	Working Experience	Core expertise	Working Experience with the firm
1.	L1 Analyst				
2.	L2 Analyst				
3	L3 SOC Specialist				
4	L1 Consultant GRC (Governance, risk management, and compliance)Team				
5	L2 Consultant GRC (Governance, risk management, and compliance)Team				
6	L1 Engineer Tools Management				
7	L2 Engineer Tools Management				
8	L2 Engineer Application and Network Security				

3I. SUMMARY OF TENDERER ANNUAL TURNOVER :

Name of the Tenderer	Turnover of the Tenderer				
	2020-21	2021-22	2022-23	2023-24	2024-25

3J : SUMMARY OF TENDERER WORK EXPERIENCE/QUALIFICATIONS :

Sl. no	Name of the Tenderer	Name of the Employer	Name of the projects completed in the last 5 years	Award reference (date & No.)	Value of the contract in INR Crores	Value of the project in INR in Crores	Date of commencement	Date of completion
1								
2								
3								
4								
5								
6								
7								

3K. AFFIDAVIT REGARDING CORRECTNESS OF INFORMATION FURNISHED AND DOCUMENTS SUBMITTED (In an appropriate value of stamp paper)

I/We…… residing at ……(*Address*)Authorized Signatory/Proprietor /Partner/ Director of M/s……situated at …… …… (*Address)* hereby solemnly declare as under:

1. That I/We have submitted my/our tender for …… in response to Invitation to Tender No……issued by …… on the KPP portal.
2. That I/We have uploaded the scanned copies/copies of the following documents as required by the tender document and in support of my meeting the stipulated eligibility and qualification requirements as stipulated in the tender document:
   (a)……
   (b) ……
   (c) ……
   (d) ……
   (e) ……
   (f) ……
3. That the information furnished by me/us in the format are correct to the best of my knowledge and the documents/ certificates uploaded are true to the originals;
4. That I/We am in possession of the original documents and ready to produce the original documents and the original documents in support of the qualification information furnished for verification by the Employer or his authorized representative within 5 days of receiving the request from the Employer or his authorized representative;
5. That I/We have not made misleading or false representation in the Forms, Statements and Attachments submitted/uploaded in proof of qualification requirements;
6. That I/We do not have record of poor performance such as abandoning the works, not properly completing the contracts, inordinate delays in completion in completion, litigation history or financial failures etc,

Authorized Signature [In full and initials]: _____
Name and Title of Signatory: _____
Name of Tenderer: _____
Address:

3L. Technical compliance of the tools/platform proposed for assessment

Tenderer to give technical compliance for all the tools specifications mentioned in Detailed Scope of work of this tender document regarding the features of the Platform or Product suggested as part of the Bid response.

SECTION-4. FINANCIAL BID – STANDARD FORMS
(Not to be disclosed in the technical part)

4A. Financial Bid submission form.

4A. FINANCIAL BID SUBMISSION FORM

(To be uploaded in the KPP portal)

[*Location, Date*]

FROM: (Name of Tenderer)

To,

The General Manager (Ele),
DAS, SG&TIC,
Corporate office, BESCOM,
K.R Circle, Bangalore.

Sir,

Subject: "**Implementation of Cyber – Security Operations Centre (C-SOC) in BESCOM (Tender No. BESCOM/2025-26/SE0441)**"– Regarding Financial Bid.

We, the undersigned offer to provide the services for the above in accordance with your Request for Bid. Our Financial bid is submitted on KPP portal in the Financial bid.

Our financial bid shall be binding upon us subject to the modifications resulting from contract negotiations, up to expiry of the validity period of the bid.

We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".

Yours sincerely,

Authorized Signature [In full and initials]: _____
Name and Title of Signatory: _____
Name of Tenderer: _____
Address: _____

SECTION 5: DETAILED SCOPE OF WORK

1. Project Background

1.1. Bangalore Electricity Supply Company Limited (BESCOM) is entrusted with the distribution of electricity across eight districts of Karnataka, covering an operational area of **41,092 square kilometers** and serving a population of over **20.7 million citizens**. BESCOM operates through:

- **4 Zones** – Bangalore Metropolitan Area Zone (North), Bangalore Metropolitan Area Zone (South), Bangalore Rural Area Zone, and Chitradurga Zone.
- **9 Circles**, **32 Divisions**, **147 Sub-Divisions**, and **534 Section Offices**.

1.2. In view of the increasing cyber threat landscape and the need for robust protection of BESCOM's digital infrastructure, there is a critical requirement to establish an integrated and next-generation **Cyber Security Operations Centre (C-SOC)** at BESCOM's premises.

2. Objectives of the Project

2.1. The proposed C-SOC (Cyber Security Operations Centre) architecture shall provide centralized cybersecurity monitoring for IT, OT, and IoT Systems, Web and Mobile Applications of BESCOM environments through a layered, DMZ-based design ensuring strict IT-OT segregation. SIEM and SOAR platforms shall be deployed in separate and dedicated instances for IT and OT environments to ensure strict segregation, independent monitoring, and controlled incident response across enterprise IT and operational technology networks.

2.2. The implementation of C-SOC will ensure:

- Real time monitoring of all logs with log aggregation having SIEM & SOAR to collect & monitor logs effectively. And analysis can be done to identify, respond and mitigate from cyber incidents.
- To provide secure storage and transfer of data, appropriate access rights to information.
- The C-SOC shall utilize NG-SIEM, SOAR, UEBA, NBAD, DAM, DDoS etc. platforms and other tools with controlled, secure, and encrypted data flow from end-points and operational systems, ensuring compliance with CEA and CERT-In guidelines while maintaining operational safety of power distribution systems conforming to technical specifications.
- To integrate proactive threat intelligence from trusted national and global sources to enable early warning, threat hunting, and predictive cyber defense.

- Governance, risk management, and compliance (GRC) by aligning with ISO/IEC 27001:2022**,** NIST Cybersecurity Framework (CSF)**,** CERT-In advisories and CEA Cyber Security Guidelines 2021 or latest.

3. Contract Period: "Implementation of Cyber - Security Operations Centre (C-SOC) in BESCOM" for a period of six-months implementation period and annual maintenance for a period of 5 years. The maintenance phase of 5 years will start after the six-months implementation period from the date of go-live (which includes complete integration of all tools and technologies to all the IT/OT/IoT applications, web and mobile applications of BESCOM) from BESCOM.

C-SOC (Cyber Security Operations Centre) architecture shall provide centralized cybersecurity monitoring for IT, OT, and IoT Systems, Web and Mobile Applications of BESCOM environments through a layered, DMZ-based design ensuring strict IT-OT segregation.

4. Scope of Works for Implementation Phase:

4.1 Design, Deployment, Commissioning, and Operation of BESCOM Cyber Security Operations Center (C-SOC)

The selected Tenderer shall be responsible for end-to-end design, deployment, commissioning, and operational readiness of a Cyber Security Operations Center (C-SOC) at BESCOM premises. The scope encompasses people, processes, and technology across BESCOM's IT, OT, IoT, and cloud environments, ensuring a fully functional and integrated security operations capability.

The team should comprise of selected tenderer's and OEM/OEM Certified resources for implementation of project. The implementation team will be responsible for design, delivery, implementation, integration, fine tuning, drafting and executing test cases and supporting UAT, and other activities required during implementation phase.

The primary responsibilities of implementation team are given below but not limited to:

a) Lead implementation effort.
b) Primarily accountable for successful implementation of the project across BESCOM.
c) Act to remove critical project bottlenecks.
d) Identification of working team members and team leads.
e) Single point of contact for BESCOM's senior management.
f) Ensure implementation timelines are met to achieve desired result.
g) Preparation and submission of Design Documents and Plan Documents
h) Monitor Change management activities during implementation.
i) Identify and implement best practices across BESCOM.

j) Co-ordinate with OEM/OEMs for successful implementation of solutions.
k) Periodic reporting to BESCOM on the implementation status, issues/ challenges faced and how these are handled.
l) Preparation of SOPs, documents, design diagrams etc.
m) Successfully complete the handover of operations to operations/monitoring team

4.2 Stakeholder Coordination and Architecture Design:

a. Comprehensive Stakeholder Engagement: The tenderer shall engage with all BESCOM business units, IT, OT, IoT, mobile and web applications stakeholder, as well as relevant external respective service providers, to capture detailed requirements, dependencies, and integration points.

b. Detailed Design & Documentation: The tenderer shall develop High-Level Design (HLD) and Low-Level Design (LLD) documents covering security solution architecture, network and data flow diagrams, use-case mapping, log source onboarding plans, and inter-system dependencies in co-ordination with BESCOM.

c. Holistic Data Flow Mapping: The tenderer shall identify trust zones, critical assets, and communication channels across BESCOM's infrastructure to ensure 100% coverage by monitoring systems.

d. Interfacing with Existing and Future Vendors Applications/IT-OT systems: The tenderer shall co-ordinate with current and future OEMs, system integrators, and managed service providers to ensure seamless interoperability of security solutions with production systems in co-ordination with BESCOM.

e. Validation and Assurance: The tenderer shall conduct design reviews, integration testing, and User Acceptance Testing (UAT) to confirm that solutions meet BESCOM's operational, regulatory, and performance requirements before production rollout as per the test cases designed on mutual consent with BESCOM and service e provider.

4.3 C-SOC Operations Room Setup

BESCOM shall allocate a dedicated, secured space within its premises for the implementation of the Cyber Security Operations Centre (C-SOC) Operations Room. The successful tenderer shall be responsible for implementing the C-SOC setup in accordance with the following specifications and requirements:

a) Operational setup of the C-SOC, including workstations, video wall displays, and seating arrangements is as per the approved layout by BESCOM. Tenderer shall provide the modular office furniture, including Ergonomically designed desks and chairs.

b) Dedicated workstations for Level-1 (L1) and Level-2 (L2) Security Analysts, L3 SOC Specialist, L1 & L2 Analyst for Governance Risk & Compliance matters. L1, L2 & L3 Analyst for tools management (EDR, DAM, EAM) for a total of fifteen (15) personnel.

c) Incident Discussion room setup including a meeting table with chairs (6 seats plus 1 executive chair), a 65″ display TV and interactive writing/whiteboard capability, and a multifunction colour printer supporting all types of sheets is to be provisioned.

d) Video Wall & Display Systems: A high-definition, multi-screen Video Wall Display System (2x2, 55 inch) to enable real-time visualization of Dashboard. The video wall shall support flexible content management, multiple input sources, and centralized control for dynamic monitoring requirements.

e) All the materials to be supplied as per the Clause 8 of Section 7, BoQ (Bill of Quantities) of this tender document.

f) Electrical and Structured Cabling: Sufficient electrical outlets and power distribution units (PDUs) to support all equipment within the C-SOC room. Structured LAN cabling (Category 6 or higher) for interconnection of all end-user systems and network components. Proper earthing /grounding, surge protection, and adherence to IS/BIS electrical safety standards.

g) Server Room Setup and Backend Infrastructure - A separate, access-controlled server room shall be designated within the BESCOM premises to house the backend infrastructure supporting the C-SOC.

   The tenderer shall install and configure all server-side components in accordance with the following technical provisions:

   i.) Rack Space and Equipment Mounting: BESCOM shall provide sufficient standard equipment racks with cable organizers, PDUs, and blanking panels as required.

   ii.) The racks shall accommodate all active and passive components such as Servers (Application, Database, SIEM, Log Collector), Storage arrays, Firewalls, routers, and switches, Load balancers and other network/security appliances.

h) Network and Connectivity

   i. Dedicated MPLS connectivity (primary and secondary) with adequate bandwidth (as per the tenderer's proposed architecture) for secure, high-speed data communication.

   ii. Redundant internet leased lines for external threat intelligence feeds and remote monitoring.

   iii. Network and Security Appliances: The server room shall accommodate and support the deployment of following components

(to be supplied, configured, and maintained by the tenderer as per BoQ): Next-Generation Firewalls (NGFW) with UTM features, Intrusion Detection and Prevention Systems (IDPS), Layer 2 / Layer 3 Switches, Network Load Balancers, VPN Gateways and other edge security devices

i) Physical and Logical Security: The C-SOC room shall be secured with:

   i. Access control systems (biometric/RFID) for role-based entry authorization.

   ii. Surveillance systems (CCTV) with 30-day recording retention and centralized monitoring.

   iii. Fire detection and suppression systems (e.g., FM200 or Novec 1230-based clean agent systems) conforming to relevant NFPA/IS standards.

Sl No.	Deliverables	Quantity
1	High end configuration LINUX Consoles/PCs for L1/L2/L3/SOC team Specifications: CPU (Processor) — Power & Parallelism; AMD Ryzen 9 7950X3D or AMD Ryzen Threadripper PRO 7955WX Motherboard- For AMD Ryzen: X670E / B650E chipset; For Threadripper PRO: WRX80 chipset Storage Primary (OS + Apps): 2 TB NVMe SSD (PCIe 4.0/5.0) Secondary (Workspace / Projects): 4 TB NVMe or SATA SSD Memory (RAM): 64 GB DDR5-6000+ (minimum); 128 GB DDR5 Networking: Dual-band Wi-Fi 6E + Bluetooth 5.3 (optional based on preference); 1 GbE or 2.5 GbE onboard LAN	15 nos.
2	Chairs	15 Nos.
3	Centralized AC	2 nos.
4	High-end configuration Laptops with touch screen for CISO team Specifications: Processor (CPU) - Intel Core Ultra 7 / Ultra 9 AMD Ryzen AI 9 or high-end HX series, Storage- 1 TB NVMe SSD or larger, Display- 14″–16″ touchscreen with OLED / high-res panel Memory (RAM)- 32 GB or more	2 nos.
5	High-end configuration Laptops with touch screen for SOC team Specifications:	3 nos.

	Processor (CPU) - Intel Core Ultra 7 / Ultra 9 AMD Ryzen AI 9 or high-end HX series, Storage- 1 TB NVMe SSD or larger, Display- 14″–16″ touchscreen with OLED / high-res panel Memory (RAM)- 32 GB or more	
6	Printer (Multi-functional) with colour	1 no.
7	Executive Chairs for Incident discussion Room	6 nos.
8	Incident discussion Table	1 no.
9	TV - 65 inches for Discussion Room	1 no.
10	Writing board	1 no.

4.4 Deployment of Security Tools and Technologies:

a) Security Information & Event Management (SIEM)

- Deploy and configure a SIEM platform for real-time security monitoring.
- Onboard logs from critical IT, OT, IoT, network devices, applications, cloud environments, and other relevant assets.
- Implement log normalization, correlation rules, and dashboards for incident detection, threat analysis, and compliance reporting aligned with ISO/IEC 27001 and CERT-In advisories.
- Develop initial use cases for automated detection of security incidents.

b) Security Orchestration, Automation, and Response (SOAR)

- Deploy a SOAR platform to automate repetitive SOC workflows and orchestrate security tool responses.
- Develop and implement incident response playbooks for malware, phishing, insider threats, and OT anomalies.
- Integrate SOAR with SIEM, firewalls, EDR, ticketing systems, and threat intelligence platforms for automated and semi-automated responses.

c) Threat Intelligence Platform (TIP)

- Implement a centralized TIP to aggregate threat feeds from open-source, commercial, and CERT-In sources.
- Correlate threat intelligence with SIEM events to provide enriched alerts.
- Establish procedures for proactive threat hunting and periodic threat landscape assessment.

d) Endpoint Detection & Response (EDR)

- Deploy EDR agents across all enterprise endpoints, servers, and critical OT systems.
- Configure policies for behavioral analysis, anomaly detection, forensic data capture, and endpoint isolation.

e) Database Activity Monitoring (DAM)

- Implement a DAM solution to monitor, detect, and alert on unauthorized or anomalous database activity across critical systems.
- Integrate DAM logs and alerts with the SIEM for centralized visibility and correlation with other security events.
- Configure activity monitoring for sensitive data access, privilege misuse, and potential insider threats.

f) Network Behavior Anomaly Detection (NBAD)

- Deploy NBAD solutions to identify unusual network traffic patterns indicative of threats or malicious activity.
- Integrate NBAD alerts into the SIEM for correlation and proactive threat detection.
- Establish baselines for normal network behavior and continuously update detection models to adapt to emerging threats.

g) Vulnerability Management (VM)

- Implement a comprehensive vulnerability scanning solution covering IT, OT, IoT, and cloud systems.
- Conduct baseline scans, identify vulnerabilities, provide remediation recommendations, and integrate VM results with the SIEM for continuous monitoring.

h) Mobile Application Security (RASP)

- Integrate Runtime Application Self-Protection (RASP) for BESCOM's mobile applications.
- Enable detection of runtime threats, including tampering, reverse engineering, malicious code injection, and API misuse.

i) Infrastructure and Cloud Onboarding

- Onboard BESCOM's on-premises and cloud infrastructure (private and public) into the SOC monitoring framework.
- Configure connectors, APIs, and telemetry to achieve unified monitoring, alerting, and compliance visibility.

j) External Attack Surface Management (EASM)

- Identify and monitor BESCOM's external-facing assets, including domains, IPs, and web services.
- Detect shadow IT, misconfigurations, certificate expirations, and exposed data.
- Integrate findings with SIEM for continuous risk assessment.

k) DDoS Protection

- Implement a hybrid (cloud + on-premises) DDoS mitigation solution.
- Configure detection and scrubbing mechanisms for volumetric, protocol, and application-layer attacks.
- Integrate monitoring and reporting with SOC dashboards.

l) Web Application Firewall (WAF) and API Security

- Deploy WAF to safeguard web portals, APIs, and mobile backends.
- Enable virtual patching, bot mitigation, and protection against OWASP Top-10 threats.
- Configure alerting and reporting integration with SIEM.

m) Unified Endpoint Management (UEM)

- Onboard enterprise desktops, laptops, and mobile devices into the UEM solution.

- Enforce patch compliance, encryption, remote wipe, and security baselines.

- Integrate UEM alerts with SOC monitoring.

n) Identity and Access Management (IAM) Integration

- Integrate Single Sign-On (SSO) with enterprise AD/LDAP or Identity Provider.

- Implement Multi-Factor Authentication (MFA) and role-based access for all administrative accounts.

- Deploy Privileged Access Management (PAM) to monitor and control administrator activity.

o) Ticketing Tool – ITSM and ITAM

The proposed IT Service Management (**ITSM**) and IT Asset Management (**ITAM**) solution shall comprehensively address end-to-end service management, asset governance, and operational workflow requirements across BESCOM. The solution shall be uniformly adopted for all ongoing and future BESCOM projects, including the proposed Cyber Security Operations Centre (CSOC). The core functionalities expected from the selected tenderer include, but are not limited to, the following:

- Service Desk & Ticketing: Centralized helpdesk with multi-channel ticket creation (email, portal, SMS, API, chatbot, operator-assisted, etc.). Support for automated ticket categorization, prioritization, assignment, and escalation.

- Incident, Problem, and Change Management: Structured workflows for managing the complete lifecycle of incidents, problems, and changes. Root cause analysis (RCA) integration, approval processes, etc..

- Alignment with ITIL v4 best practices for stability, predictability, and controlled change implementation.

- SLA Management: Configuration and tracking of Service Level Agreements (SLAs) across all service categories. Automated SLA violation alerts, performance reporting, and dashboard visibility for BESCOM and other project stakeholders.

- Hardware & Software Asset Management (ITAM): End-to-end tracking of physical and logical assets, including procurement, deployment, utilization, maintenance, and retirement, License and compliance monitoring for software products and security platforms.

- Known Error Database (KEDB) Management: Repository for recurring issues, known errors, workarounds, and preventive measures to reduce mean time to resolve (MTTR) and improve service quality.

- The solution must support automated asset discovery using network scanning, agent-based and agent-less discovery mechanisms, as well as interrogation of cloud, virtualized, and OT environments wherever applicable. The solution shall maintain an updated asset inventory while also supporting manual data entry for exceptional cases.

- The solution shall be fully compliant with ITIL v4 standards and shall include industry-standard, pre-configured workflows for all major ITSM processes. Additionally, the solution must provide provisions for designing customizable workflows to align with BESCOM's operational and regulatory requirements.

- The selected tenderer shall be responsible for configuring, customizing, and operationalizing all required workflows pertaining to incident, ticket, change, problem, and release management. The tenderer shall also configure, monitor, and continuously track SLA and OLA parameters applicable to the NGSOC. This includes dashboard creation, periodic reporting, and integration of SLA metrics with BESCOM's governance framework.

4.5 Outline of Tasks to be Carried Out Under Implementation of C-SOC:

The successful tenderer shall undertake end-to-end planning, design, deployment, integration, commissioning, and operational enablement of the BESCOM Cyber Security Operations Centre (C-SOC). The scope of activities shall be carried out in a methodical, standards-aligned, and auditable manner, covering all phases from requirement gathering through steady-state operations. The tenderer is expected to do following but not limited to:

- Supply, design, implement, management and monitor C-SOC other security solutions.
- Security monitoring of attacks into/on/against BESCOM's IT/OT/IoT assets and data.
- Manage security, configuration, availability, performance and fault management, advisory for the security devices and its software stipulated in scope.
- Provide total anti-phishing, brand monitoring services for BESCOM and BESCOM 's internet facing IT/OT/IoT web and mobile applications.
- Design and implement security orchestration by integrating various security devices and sharing threat intelligence feeds among them.
- Design, implementation of detailed threat modelling, use cases and improving the same on continuous basis.
- Design, build, configure and manage the AI/ML models along with integration of necessary source logs for effective monitoring of BESCOM's security posture on a proactive basis.

- Provide proactive threat intelligence and perform threat hunting by building hypothesis.
- Assessment of threat intelligence feeds for their effectiveness and efficiency on regular basis and changing threat intelligence feeds provider if required.
- Ensure malware scanning, protection, presentation, and reporting as required by BESCOM.
- Risk assessment and mitigation, protection, execution support for the security solutions, devices, software and applications under the scope of C-SOC.
- Provide forensics/incident response support as per the requirement of BESCOM in case of any incident.
- Build a custom CISO dashboard, Executive dashboard as per the requirement of BESCOM to provide the high level and complete overview of BESCOM's security landscape.
- Dashboard for reporting and SLA management.
- Monitoring entire network, links, systems, devices, applications, etc. for availability, performance, SLA and other parameters using tools.
- Provide helpdesk, ticketing tools to facilitate proper governance of helpdesk activities.
- Manage and maintain all the proposed security devices/solutions with the help of dedicated onsite team.
- Fix and comply with all the audit and VAPT observations with respect to C-SOC and other security solutions in a time bound manner.

4.6 Functional Requirement of Tools and Technologies:

The C-SOC dashboard shall include, but not be limited to, the following features:

a. Real-Time Monitoring & Visualization
b. Live data feeds from SIEM and other integrated systems with refresh interval ≤ 30 seconds.
c. Role-based dashboards with tailored views for Analysts, SOC Managers, CISO, and BESCOM Board/Leadership.
d. Incident Heat maps showing geographic distribution of alerts (e.g., by division/zone).
e. Trend Analysis with historical views (hourly, daily, weekly, monthly).
f. Asset Risk Scoring showing critical assets at risk based on vulnerabilities and active threats.
g. Business Impact Indicators mapping incidents to applications and critical services from the Hosting Matrix.
h. All the solutions proposed as part of this project should have uptime as mentioned in SLA.
i. All tools, licenses and subscriptions to be taken in the name of BESCOM

4.7 General Requirements:

- The selected tenderer should perform integration of CSOC with existing BESCOM IT/OT/IoT network, mobile, web applications, applications/services hosted in public cloud and security solutions of BESCOM. The selected tenderer is also responsible for any future integrations post final acceptance at no additional cost to BESCOM.

- Conducting regular DC-DR drills for the proposed solutions. The periodicity of the PDC-DR drill shall be twice a year.

- The selected tenderer is responsible for taking regular backups and restoration of backup whenever required.

- The selected tenderer should carryout hardening of servers, OS, applications, fixing of bugs and configuration checks before Go-live of the solutions and on regular basis after Go-live and final acceptance of the solution.

- The tenderer is responsible for all aspects of the project including site survey, feasibility analysis, delivery, installation, configuration, integration, migration, conducting QA, assisting UAT, commissioning and providing on-site support during the contract period. Tenderer is also responsible for timely implementation of version upgrade, updates and bug fixes of the supplied system as and when they are available from the OEM.

- Tenderer shall provide and install necessary public Digital certificates (if applicable) on the proposed solution wherever required both at DC and DR which shall be valid for complete duration of the contract.

- The selected tenderer should carryout thorough security check for architecture flaws, misconfigurations, authentications, authorization, access related issues before Go-live of the solution. Tenderers should submit a report in this regard.

- All the tools supplied as part of the project should be supplied with Enterprise grade Licenses and all the licenses should be in the name of BESCOM. BESCOM should have the right to use the tools for the functions provided by the tools in any manner. For all the proposed tools, technologies, services etc. the enterprise support with highest level category/tier/etc. should be taken.

- The architecture should be vetted by respective OEM and implementation to be done post approval from BESCOM. Post installation, OEM should audit the configurations, policies, deployment architecture etc. and should submit the certificate that the installation was done as per the standard and best practices of OEM. The final acceptance will be issued only post the OEM audit and certification.

- All the technologies/solutions proposed under this project should have in-built AI/ & ML capabilities that significantly enhance the solution's ability to detect, prevent and respond to modern day cybersecurity threats.

- If the solution provider/tenderer lacks the expertise for a particular in-scope tool, then the OEM should provide implementation and professional services or support, for its own solution, on behalf of the solution provider/tenderer, without any extra cost.

- Versions, Upgrades and Updates: All patches, upgrades, updates of software components should be provided during the entire tenure of the agreement. The Tenderer should quote all the latest versions (current line) of products, software, hardware, servers and appliances. The quoted products, software, hardware, servers, appliances should not be declared as end of support during the period of agreement.

- Tenderer should quote the entire necessary infrastructure/software/any other component as may be required to implement the proposed solution. In case the tenderer has not indicated any peripherals/ software /equipment/plug-in/hardware in their proposed solution and are required for implementation of solution, tenderer has to provide required peripherals/ software / equipment without charging any extra amount to BESCOM.

- The technical sizing mentioned in RFP for all products/solutions (including network security technologies) are indicative and tenderers should do their assessment and quote accordingly to meet the functional specifications given by BESCOM.

- The selected tenderer should upgrade entire solution to one stable higher version till the end of Contract Period.

- Back-to-Back OEM support: The back to back OEM support for all the supplied solutions should be available for all the proposed components during the contract period (5 years from final acceptance of the solution). Tenderer should engage OEM for each and every technology solution proposed and OEM should certify that the implementation done by tenderer is as per industry standard and best practices followed for that particular technology domain. The OEM should also certify that the products supplied as part of this project should be supported throughout the tenure of the contract.

- Prior to bidding, the tenderer should conduct site survey of the data centre, SOC room, and suggest BESCOM the infrastructure requirements including but not limited to power requirement, cooling requirement, internet bandwidth requirement etc. and should submit a certificate confirming the same.

- The tenderer should execute a Confidentiality and Non-Disclosure Agreement as also an Undertaking inter alia that they shall not disclose any information acquired while dealing with the Project which is confidential in nature to anybody including their relatives.

- The tenderer should perform their own feasibility, groundwork etc. in order to quote for the necessary components for the solution in order to ensure that the solution to work as per the functional, technical and general specifications mentioned in the RFP.

- Any solution/ technology/service which is not performing as per functional and technical requirements of this tender document or not giving the desired output/performance, the tenderer shall replace the solution/ technology at no cost to BESCOM during the contract period.

- Any solution/ technology/service which is impacted due to merger/ acquisition/ closure/ partial closure/etc. of the OEMs, tenderer shall replace the solution/ technology at no cost to BESCOM during the contract period without any disruption to the services of BESCOM.

- If tenderer is unable to provide support or any solution component of hardware and software goes end of support during the validity of the contract or upgrade for any of the components is needed for any newly emerged threat/vulnerabilities, then the

Tenderer shall upgrade the component/ sub-component with an alternative that is acceptable to BESCOM at no additional cost to BESCOM and without causing any performance degradation and/or project delays.

- As per BESCOMs requirement, the successful tenderer of the project should be ready to shift, occasionally, the equipment from one place to other, uninstall and reinstall all the equipment without any additional cost to BESCOM.

- The tenderer shall manage the overall infrastructure comprising of all deployed solutions and the associated infrastructure such that an infrastructure uptime on a quarterly basis, shall be maintained in accordance with SLA terms of this tender document.

- All the supplied systems should be covered under warranty for 5 years from date of final acceptance. Warranty charges should cover product/solution version upgrade (to the latest available version for supplied systems), updates and bug-fixes and its implementation during the contract period.
- OEM support services on 24 x 7 x 365 days basis should be provided for problem resolutions and OEM technical expert shall provide onsite support as and when required for maintaining the uptime and SLA requirements during the warranty.

- Technical literature or any other support related to the supplied solutions shall also need to be provided as and when required for the proper functioning of the systems. These warranty services will be provided to BESCOM without additional cost other than the warranty charges.

- The Tenderer should ensure the proposed solutions should be compatible with or able to integrate with quantum-resistant technologies and encryption methods whenever BESCOM requires to do so.

- The tenderer should ensure the proposed solutions should be flexible enough to integrate with new technologies and standards as they emerge.

- Tenderer should bring all the tools and equipment (Including cables, SFP, transceivers) for successful commissioning of hardware and software for successful implementation of Solution. Tenderer should bring all the tools and equipment

(Including cables, SFP, transceivers) for successful commissioning of hardware and software for successful implementation of Solution.

- The Tenderer would be the single point of contact for any matters requiring OEM support. The Tenderer should have back-to-back agreements with respective OEMs to ensure onsite support for each solution.

- The Tenderer should size the hardware/appliance/storage as per the requirements of RFP document. The Tenderer's response should include the calculations / logic used to arrive at the sizing. In case any further clarification related to the sizing of hardware is required, Tenderer can consult BESCOM and seek clarification. The performance and hardware sizing should be done as per the requirements of RFP and should not underperform during the contract period. In case of any underperformance the tenderer should upgrade/resolve the performance issues at no cost to BESCOM throughout the contract period.

- The uptime and downtime of the software's/tools shall be recorded with reasons and submit to the BESCOM to avoid the penalty.

- The bidder shall comply with all applicable provisions, amendments, advisories, directions, and guidelines issued by NCIIPC, CEA, CERT-In, and under the Information Technology Act, 2000 (including all rules and amendments thereto), as applicable, throughout the entire contract period.

- Data Protection & Privacy: All data generated, accessed, or processed under the SOC shall remain the exclusive property of BESCOM and shall be stored and processed within India in compliance with applicable laws including IT Act 2000 and DPDP Act 2023. The bidder shall ensure confidentiality, implement adequate security controls, and restrict data usage strictly to contract purposes. Any data breach shall be reported immediately, and data shall be securely handed over and destroyed upon contract termination.

5. Human Resource Details:

5.1. The resources provided by tenderer should be deployed completely onsite at BESCOM locations. The resources deployed for this project should be on the payrolls of tenderer. The minimum resource requirement at various stages of the project are given in RFP.

5.2. Tenderer is required to provide experienced and certified manpower as mentioned in RFP.

5.3. While BESCOM has mentioned the minimum resources that need to be deployed, tenderer may propose additional resources as per their assessment to meet SLA requirements. However, the SLA on manpower deployed will be only on the proposed manpower as per the BoM.

5.4. The resources deployed shall mandatorily record attendance in BESCOM installed attendance system.

5.5. On-Site Resource Deployment and SOC Operations Requirements: To ensure uninterrupted, SLA-compliant Security Operations Center (SOC) services, the successful tenderer shall deploy an appropriate number of skilled and qualified resources on-site, with adherence to BESCOM's standards, policies, procedures, and processes.

5.6. The Operations team should be deployed prior to final acceptance of solution in order to ensure smooth transition.

- The operations team is responsible for day-to-day maintenance of entire setup and adhering with SLA terms, smooth transition of operations from implementation team.
- The Operations Teams should work in a cohesive manner to ensure the Security of BESCOM is prioritized without any delay.
- The Operations team are expected to extend the required assistance as and when requested by BESCOM Officials.

5.7. Resource Deployment Guidelines: The tenderer shall permanently depute a team of qualified, trained, and certified professionals at BESCOM premises (or as per requirement).

5.8. Minimum manpower deployment shall be as follow:

5.8.1. **SOC Team:**

a) L1 SOC Analysts – 06 Nos (on-site, 24×7×365 rotational shifts)

b) L2 Senior SOC Analysts – 03 Nos (on-site, 24×7×365 rotational shifts)

c) L3 SOC Specialist – 01 No (onsite dedicated resource 24×7×365 availability for escalations and critical support)

5.8.2. **GRC (**Governance, risk management, and compliance**) Team:**

a) L1 Analyst – 1No – General Shift

b) L2 Analyst – 1No – General Shift

5.8.3. **Tools and Management team**

a) L1 Analyst – 1No – General Shift

b) L2 Analyst – 2 Nos – General Shift

Note: Onsite dedicated resource must be 24×7 available for escalations and critical support when required.

5.9. Shift Coverage and Continuity: The SOC operations team shall provide round-the-clock (24×7×365) monitoring of tools, man the helpdesk, and execute daily SOC operations as per industry best practices. Adequate backup resources must be available to ensure continuity in case of absence/leave of regular staff, without any service disruption.

5.10. **Scope of Responsibilities:** The deployed team shall be responsible for:

i. Continuous monitoring of SIEM, SOAR, UEBA, NBAD, EDR, DAM, WAF, RASP
ii. tools.
iii. Threat hunting, threat intelligence integration, and analytics-based detection.
iv. Incident triage, containment, eradication, and response as per SOPs.
v. Proactive advisory on security incidents, threats, and emerging risks.
vi. Generation of daily, weekly, and monthly operational reports and dashboards.
vii. Supporting audits, compliance reporting, and regulatory obligations (e.g., CERT-In timelines).
viii. Maintaining and tuning detection rules, playbooks, and escalation workflows.
ix. Governance, Compliance, and Replacement

5.11. BESCOM reserves the right to interview and approve resources prior to their onboarding.

5.12. BESCOM may request replacement of resources in case of unsatisfactory performance; the tenderer shall provide a replacement within seven (7) days.

5.13. The tenderer shall provide Background Verification Reports (BVR) for all deployed manpower and ensure execution of Non-Disclosure Agreements (NDA) before deployment.

5.14. Operational Discipline and Documentation:

I. All backup resources shall be periodically updated and trained to ensure they remain familiar with BESCOM's IT security environment and ready to take over duties at any time.
II. The tenderer shall maintain detailed runbooks, SOPs, and knowledge bases for all SOC activities.

5.15. Commercial Commitment: The manpower cost quoted in the Final Commercial Bill of Materials shall be treated as fixed for the entire contract term. Partial deployment of resources is strictly prohibited.

5.16. **Post-Contract Emergency Support**: The tenderer shall provide emergency support even beyond the contract period (Five years after Go-Live) until BESCOM transitions to a new service provider or in-house operations.

5.17. **General requirement of all resources:**

I. In case of exigencies, L1, L2 and L3 shall be available after business hours and on Sundays and Holidays as well.

II. The SOC Manager shall ensure that adequate human resource is available to meet the deliverables as per the scope of work and maintain performance and availability requirements as per SLA.

III. All the relevant documentation including SOPs, workflows, manuals etc. need to be updated by the team in coordination with the BESCOM, OEM & Tenderer from time to time.

IV. Regular training and knowledge updates/ sessions / refreshers shall be imparted by the tenderer to the support team in coordination with SME from OEM(s) throughout the contract period which shall be reviewed periodically by BESCOM

V. The SOC Manager shall report the profile, attendance details, key resource and responsibilities and any other details of the team deemed necessary to a SPOC identified from BESCOM

VI. BESCOM reserves the right to periodically review the performance of the tenderer/OEM and its employees under the managed services and may ask for replacements if required. BESCOM shall increase or decrease the number of resources at any stage if required.

VII. The selected tenderer shall ensure that proposed team is competent, professional and possess requisite qualifications and experience appropriate to the task they are required to perform under the scope of services and FMS qualifications defined in this RFP.

5.18. **Human Resource Deployment Matrix with Shift Coverage**

5.18.1. The SOC shall operate in a 24×7×365 environment with a 3-shift model (8 hours per shift). The minimum resource distribution across shifts shall be as follows:

Role	Total Nos.	Shift Coverage (24×7)	Per Shift Deployment	Minimum Qualifications & Certifications	Remarks
L1 SOC Analyst	**06**	3 Shifts (A,B,C)	**2 nos.**	**Education:** BE/BTech/BCA/MCA in CS/IT/ECE/Cyber Security. **Certifications:** CEH/CompTIA Security+ (mandatory). **Experience:** ≥2 years SOC operations experience handling SIEM, UEBA, EDR tools, log management, incident triage.	Responsible for real-time monitoring, alert triage, ticket creation, correlation rule tuning, and L1 escalations.
L2 Sr. SOC Analyst	**03**	3 Shifts (A,B,C)	**1 no.**	**Education:** BE/BTech/BCA/MCA in CS/IT/ECE/Cyber Security. **Certifications:** OEM product certifications (SIEM/EDR), GCIA/GCIH, or equivalent. **Experience:** 3–5 years SOC experience; must have handled escalations from L1 team for at least 2 years.	Performs in-depth incident investigations, develops new correlation rules/parsers, leads incident response at L2, mentors L1 analysts, and coordinates with IT/OT teams.
L3 SOC Specialist (Team Lead)	**01**	General Shift	**1 no.**	**Education:** BE/BTech/MCA with ≥65% marks. **Certifications:** GCFA / GCFE / CISSP / OSCP / CCIE / CEH (mandatory). **Experience:** 5-7 years SOC experience with proven expertise in incident response, digital forensics, threat hunting, and SIEM/SOAR tuning.	Leads complex investigations, threat-hunting campaigns, builds SOAR playbooks, produces KPI reports (MTTD/MTTR), and drives detection engineering. Must be reachable within 30 minutes for P1/P2 incidents.

5.18.2. **Governance Risk & Compliance Team:**

Tenderer shall manage the overall Compliance as defined in section 4.5 through 4.8 on Governance Risk & Compliance, Vulnerability Management, Business continuity & Resilience & Security Awareness & coordination.

Role	Total Nos.	Shift Coverage (8x5)	Per Shift Deployment	Minimum Qualifications & Certifications	Remarks
L1 Consultant	**1**	General Shift	**1 no.**	**Education:** BE/BTech/BCA/MCA in CS/IT/ECE/Cyber Security. **Certifications:** CEH/CompTIA Security+ (mandatory). **Experience:** ≥2 years operations experience handling Vulnerability Management tools & process.	Responsible for Vulnerability & Attack Surface Management activities.
L 2 Consultant	**1**	General Shift	**1 no.**	**Education:** BE/BTech/BCA/MCA in CS/IT/ECE/Cyber Security. **Certifications:** CEH/CompTIA Security+ / ISO 27001LA (mandatory). **Experience:** ≥3 years experience handling Compliance management & reporting.	Responsible for Compliance management & reporting.

5.18.3. **Security Device Management and Administration**

a. Tenderer shall manage the overall management of proposed security solutions/ devices as per the IS (Information Security) policy of BESCOM /statutory regulations, etc. as applicable time to time.

b. The tenderer is expected to manage the following through onsite teams

c. The selected tenderer has to perform periodic review and fine tuning of devices to fit BESCOM's network environment and requirement.

d. Device lifecycle management, License management and OEM co-ordination has to be governed by the tenderer under BESCOM's supervision.

e. The change management of all the devices, both hardware and software, must be adhering to standards and policies of BESCOM and respective SLA will be applicable to the selected tenderer.

f. In case of any hardware/software malfunctioning, patch management, firmware upgradation and other OEM related tasks of the device, the SOC team has to coordinate with the concerned OEMs of the solutions for faster resolution.

g. The team also has to monitor and report the hardware and software related SLA's of all applicable security device / solutions implemented at BESCOM.

h. The tenderer is expected to fine tune the configuration /operational /process settings based on the trends identified as part of Advanced Threat Monitoring and should be part of continuous improvement plan.

i. The team will address all the user-related issues with respect to proposed solutions in time bound manner

Role	**Total Nos.**	**Shift Coverage**	**Per Shift Deployment**	**Minimum Qualifications & Certifications**	**Remarks**
L1 Engineer (Endpoint Tools)	**1**	General Shift	**1 per shift**	**Education:** BE/BTech/BCA/MCA in CS/IT/ECE/Cyber Security. **Certifications:** CEH/CompTIA Security+ (mandatory). **Experience:** ≥2 years operations experience handling Endpoint Security & UEM	Responsible for Management & trouble-shooting of issues in EDR, DAM, UEM & IAM.
L 2 Engineer (Endpoint Tools)	**1**	General Shift	**1 per shift**	**Education:** BE/BTech/BCA/MCA in CS/IT/ECE/Cyber Security. **Certifications:** CEH/CompTIA Security+ / ISO	Responsible for Administration, Management & trouble-shooting of issues in EDR, DAM, UEM & IAM.

Role	Total Nos.	Shift Coverage	Per Shift Deployment	Minimum Qualifications & Certifications	Remarks
				27001LA (mandatory). **Experience:** ≥4 years experience handling Compliance management & reporting.	
L2 Engineer (Application & Network Security)	**1**	General Shift	**1 per shift**	**Education:** BE/BTech/BCA/MCA in CS/IT/ECE/Cyber Security. **Certifications:** Industry Certifications on WAF,DDOS **Experience:** ≥5 years experience handling Compliance management & reporting.	Responsible for Administration, Management & trouble-shooting of issues in RASP,DDOS,WAF.

5.18.4. **Shift Timing (Indicative)**

- Shift A – 06:00 hrs to 14:00 hrs
- Shift B – 14:00 hrs to 20:00 hrs
- Shift C – 20:00 hrs to 06:00 hrs
- General Shift (Business Hours) – 09:00hrs to 18:00 hrs

Note: The Tenderer shall ensure continuous manning of all shifts with no service disruption. Backup resources must be pre-trained and available to cover leaves, attrition, or emergencies.

5.18.5. **Dedicated Resource Commitment**

a. **Exclusivity**: All deployed manpower shall work exclusively for BESCOM SOC during the entire contract duration:

b. **No Resource Sharing:** Deployed resources shall not be shared with other employers/projects unless approved in writing by BESCOM.

c. **Continuity**: Replacement with equal or higher-qualified resources must be provided within 7 calendar days in case of attrition or performance issues.

d. **Knowledge Transition:** Proper documentation and periodic knowledge-transfer sessions must be conducted

to ensure smooth operations during the entire 5-year engagement.

5.18.6. **Mandatory Training & Certification**

To maintain high operational maturity and compliance with global standards, the following training and certification requirements shall be enforced:

a. **Annual Training & Refreshers**: All resources (L1, L2, L3, SOC Manager) must undergo annual OEM product refresher training on SIEM, SOAR, UEBA, NBAD, EDR, DAM, and other SOC tools deployed at BESCOM.

b. **Threat intelligence and incident response** playbook workshops must be conducted quarterly to keep the team aligned with evolving cyber threat landscape and MITRE ATT&CK updates.

c. **Certification Maintenance**: All mandatory certifications (CEH, GCIA, GCIH, CISSP, CISM, etc.) must be renewed before expiry at the tenderer's cost.BESCOM reserves the right to verify the certification status of deployed resources at any time.

d. **Cross-Training & Backup Readiness**: L1 resources must be periodically trained on L2-level tasks and tools to create a skilled backup pool .Backup resources must be familiarized with BESCOM environment through shadowing and periodic mock drills.

e. **Compliance Documentation**: The tenderer shall maintain training records, certificates, and skill-matrix documentation and share them with BESCOM during quarterly reviews and audits.

5.18.7. **Additional Compliance & Flexibility**

a. **Minimum Staffing Commitment**: The tenderer shall ensure that minimum staffing levels per shift are always met.

b. **Surge Capacity**: During major incidents, audits, or compliance cycles, tenderer shall augment manpower as needed without additional cost.

c. **Resource Governance**: BESCOM reserves the right to interview resources before deployment and seek replacement for non-performance.

5.18.8. **Post-Implementation Operations**

a. Continuous incident notification and communication with application teams.

b. Daily monitoring, reporting, and documentation of incident status, root causes, and remediation's.

c. Optimization of log queries, dashboards, and reporting for faster incident response.

d. Forensics support and threat hunting on identified incidents.

e. Periodic assessment and fine-tuning of solution configurations against global standards.

f. Proactive threat intelligence, threat actor analysis, and automated alerting for new and unknown threats.

g. Analysis of all security alerts, logs, malware, and suspicious activity from SOC tools and enterprise security devices.

h. Continuous improvement of SOC detection capabilities, rules, AI/ML models, and policies to reduce false positives.

i. Real-time situational awareness reporting to BESCOM officials.

6. The tenderer shall ensure that the salary paid to its employees should adhere to the prevailing "Minimum Wages Act 1948" throughout the contract period.

7. INDEMNITY AND VERIFICATION

Police verification certificate in respect of the candidates proposed shall be submitted by the tenderer during the selection of the candidate failing which the candidate proposed by the tenderer will not be considered. Proofs of identity like Driving License, Aadhar card, previous work experience, proof of residence and recent photograph and a certification to this effect shall be submitted to the Employer/Owner. The Tenderer shall withdraw such employees who are not found suitable by the Employer/Owner for any

reasons immediately on receipt of such a communication from the Employer/Owner. The human resources and tenderer shall execute non-disclosure agreement (NDA).

Details of Payments Receipts shall be uploaded towards payment of Professional Tax, EPF, ESI and Services taxes.

8. Insurance

8.1. The tenderer should fully insure each and every goods or products supplied under the total solution against all risks including terrorism, riots and civil commotion, etc. till the Go-Live of project with an insurance company/corporation.

8.2. In case of any loss or damage occurs, the tenderer should be responsible for initiating and pursuing claims and settlement and simultaneously also make arrangements for repair and/or replacement of any damaged item/s.

9. Continuous Security Monitoring

9.1. The C-SOC shall establish and maintain a comprehensive, always-on monitoring capability with the following key objectives and activities:

9.2. 24×7×365 Surveillance: Implement continuous, uninterrupted monitoring of BESCOM's IT, OT, IoT, and cloud infrastructure to provide real-time visibility into security events across the enterprise.

9.3. Advanced Event Detection: Detect and alert on suspicious activities, policy violations, network anomalies, privilege escalations, and Indicators of Compromise (IoCs) using automated monitoring systems.

9.4. Centralized Log Collection & Correlation: Aggregate logs from servers, endpoints, firewalls, network devices, OT controllers, IoT devices, and cloud platforms into a centralized SIEM for correlation and analysis.

9.5. Threat Intelligence Integration: Enrich security events with global, sector-specific, and CERT-In threat intelligence feeds to identify known malicious IPs, domains, hashes, and attacker TTPs (Tactics, Techniques, and Procedures).

9.6. Real-Time Event Correlation: Leverage SIEM platforms to correlate events across multiple vectors, enabling early detection of multi-stage attacks, lateral movement, and privilege misuse.

9.7. Network Behavior Anomaly Detection (NBAD): Monitor traffic baselines and flag abnormal communication patterns, beaconing activity, and potential data exfiltration attempts.

9.8. Endpoint Telemetry & EDR Monitoring: Capture endpoint behavior in real time, detect malicious processes, memory injections, and unauthorized persistence mechanisms.

9.9. Cloud Security Monitoring: Continuously monitor Cloud assets, VM's, Native Services, Applications & databases to assess attacks, malicious activities or threats.

9.10. OT & IoT Visibility: Monitor SCADA/DAS, AMI smart meters, and IoT devices for unauthorized firmware changes, communication anomalies, or cyber-physical attack attempts.

9.11. Early Warning System: Generate prioritized alerts with severity ratings and recommended response actions to facilitate quick triage by SOC analysts.

9.12. Dashboards & Situational Awareness: Provide role-based dashboards for BESCOM management and IT security teams to track live incidents, trends, and key security metrics.

9.13. Continuous Tuning & Optimization: Periodically refine detection rules, use cases, and baselines to improve accuracy, minimize false positives, and ensure coverage of emerging threats.

9.14. **Continuous security monitoring of attacks against BESCOM assets**

a. Daily CISO report shall be submitted to BESCOM in a format agreed upon and amended from time to time as per the requirements as given in RFP.
b. 24X7 log monitoring of various type of operating systems, network, security devices & solutions using SOC tools.
c. Log correlation for in depth monitoring and remedial actions on daily basis.
d. Rapid response to incidents/ alerts raised by security devices and/or monitoring systems.
e. Evaluation of incidents and implementation/recommendation of remedial measures.
f. Forensics to identify the origin of threats, mitigation thereof, initiation of logical measures to prevent recurrence, which should be acceptable to BESCOM

g. Advisories to BESCOM on relevant threats and vulnerabilities supported with mitigation against identified risk exposure
h. Continuous threat hunting activity.

10. Vulnerability management in scope of devices:

10.1. All servers, endpoints, network devices, security appliances, and virtualization platforms fall under mandatory vulnerability management scope.

10.2. The vendor shall perform authenticated scans to ensure accurate detection across all in-scope assets.

10.3. Critical infrastructure such as firewalls, routers, switches, WAF, VPN, and load balancers must be included without exception.

10.4. Scanning engines must operate fully On-Premise with no external data transmission.

10.5. The solution shall provide CVSS-based scoring and threat-contextual prioritization.

10.6. Dashboards must present real-time vulnerability exposure and device-level risk trends.

10.7. Remediation workflows shall integrate with ITSM for ticketing and closure tracking.

10.8. Monthly vulnerability assessments and quarterly deep-dive reviews must be conducted.

10.9. The vendor shall maintain a device inventory map with scan coverage and compliance status.

10.10. SLA-driven reporting must highlight critical unpatched assets, exceptions, and remediation timelines.

11. Business Continuity and Disaster Recovery Plan

11.1. The C-SOC shall play a proactive and strategic role in ensuring that BESCOM's critical services remain resilient and operational during cyber incidents, disasters, or major disruptions. The activities shall include, but not be limited to, the following:

11.2. Integration with BCP/DRP:Fully integrate SOC processes with BESCOM's Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) to ensure coordinated response during crises.

11.3. Map critical BESCOM services, dependencies, and recovery priorities to SOC monitoring and response workflows.

11.4. Technology Refresh & Optimization:

11.4.1. Review SOC tools and platforms periodically to ensure they remain current, scalable, and aligned with modern security requirements (e.g., AI/ML, SOAR enhancements, cloud-native monitoring).

11.4.2. Recommend upgrades or replacements when technologies reach end-of-support or fail to meet evolving requirements.

11.5. Executive Security Briefings: Provide quarterly executive-level briefings for BESCOM leadership, summarizing the threat landscape, incident trends, lessons learned, and recommended investments for future preparedness.

11.6. Participation in Sector-Wide Cyber Drills: Support BESCOM's participation in national/state-level cyber drills (CERT-In, NCIIPC, CEA) and incorporate lessons learned into SOC processes.

11.7. Strategic Threat Forecasting:

11.7.1. Leverage threat intelligence and predictive analytics to forecast emerging attack trends and prepare BESCOM in advance.

11.7.2. Recommend preventive measures (e.g., advanced endpoint protection, network segmentation, zero-trust architecture) to mitigate anticipated threats.

11.7.3. The C-SOC shall implement a robust, well-defined, and rapid incident response framework to ensure timely containment and resolution of security incidents, minimizing business impact. The activities shall include but not be limited to the following:

11.8. Structured Incident Triage & Classification: Establish a formalized triage process with defined severity levels (Critical, High, Medium, Low) to quickly categorize incidents based on business impact, regulatory relevance, and urgency.

11.9. Prioritization & Escalation Matrix: Develop a clear escalation hierarchy and communication workflow to ensure that high-severity incidents are immediately escalated to senior management, relevant application owners, and decision-makers.

11.10. Automation & Orchestration: Utilize SOAR (Security Orchestration, Automation, and Response) playbooks to automate repetitive tasks

such as log enrichment, containment actions, and ticket generation, thereby reducing analyst workload and human error.

11.11. Mean Time to Detect (MTTD) & Mean Time to Respond (MTTR) Reduction: Continuously monitor and improve performance metrics to ensure faster detection, triage, containment, and remediation of threats.

11.12. Rapid Containment & Eradication: Define clear procedures for quarantining infected endpoints, blocking malicious IPs/domains, disabling compromised accounts, and removing malicious artifacts from the environment.

11.13. Incident Workflow Documentation: Maintain detailed step-by-step workflow documents for common incident types (phishing, ransomware, malware outbreaks, insider threats, DDoS attacks, OT system anomalies) to ensure repeatable, consistent response actions.

11.14. Forensic Data Preservation: Collect and preserve all relevant logs, memory images, and evidence in a tamper-proof manner to support root cause analysis, regulatory reporting, and possible legal proceedings.

11.15. Communication & Notification Protocols: Implement a formal incident notification mechanism to inform BESCOM management, stakeholders, CERT-In, and regulatory bodies as per mandated timelines.

11.16. Coordination with External Agencies: Facilitate seamless collaboration with CERT-In, NCIIPC, law enforcement, and third-party vendors during major incidents or breaches.

11.17. Root Cause Analysis (RCA): Conduct detailed RCA post-resolution to identify vulnerabilities, gaps, and process failures that contributed to the incident.

11.18. Lessons Learned & Policy Updates: Document lessons learned from every major incident and update SOC processes, detection use cases, and playbooks to prevent recurrence.

11.19. Crisis Management & Tabletop Exercises: Periodically conduct tabletop simulations and mock drills (Red Team / Blue Team exercises) to test and validate BESCOM's readiness to handle large-scale incidents.

11.20. Business Continuity Support: Ensure alignment of response activities with BESCOM's Business Continuity and Disaster Recovery Plans to minimize disruption to critical operations.

12. Threat Intelligence and Proactive Defense

12.1. The C-SOC shall adopt a threat-intelligence-driven security model to stay ahead of adversaries and proactively defend BESCOM's critical infrastructure. The activities under this scope shall include the following:

12.2. Comprehensive Threat Intelligence Collection: Continuously gather and aggregate intelligence from multiple trusted sources including global threat intelligence providers, government agencies (CERT-In, NCIIPC, CSIRT-Power), Information Sharing and Analysis Centers (ISACs), and open-source intelligence (OSINT) feeds.

12.3. Normalization & Contextualization: Normalize threat data (IP addresses, domains, malware hashes, TTPs) and correlate them with BESCOM's internal telemetry to provide actionable insights.

12.4. Sector-Specific Intelligence: Focus on energy sector–specific threat advisories, attack campaigns, and emerging vulnerabilities affecting SCADA, AMI, and OT networks to ensure targeted defense.

12.5. Advanced Correlation with SIEM: Enrich SIEM alerts with threat intelligence to improve detection fidelity, reduce false positives, and highlight high-priority incidents.

12.6. Proactive Threat Hunting: Conduct continuous and scheduled hunting exercises to identify advanced persistent threats (APTs), stealthy malware, lateral movement, and early indicators of compromise before they escalate into full-blown incidents.

12.7. MITRE ATT&CK Mapping: Align threat hunting activities and detection use cases with the MITRE ATT&CK framework to cover a comprehensive range of adversary tactics and techniques.

12.8. TTP Analysis & Adversary Profiling: Analyze threat actor behavior, campaigns, and infrastructure to build Threat Models and anticipate potential attack vectors against BESCOM.

12.9. Early Warning & Advisory Dissemination: Generate actionable threat advisories and alerts for BESCOM's IT, OT, and IoT teams, ensuring timely mitigation actions are implemented.

12.10. Collaboration & Information Sharing: Participate in national cyber threat-sharing forums and collaborate with CERT-In, CEA, and other ESCOMs to exchange intelligence on ongoing attack campaigns.

12.11. Integration with SOAR & TIP: Automate ingestion and operationalization of threat intelligence in SOC workflows, enabling real-time detection and blocking of malicious indicators.

12.12. Continuous Threat Landscape Assessment: Periodically review and report on the global and domestic cyber threat landscape, highlighting trends, targeted sectors, and emerging attack vectors relevant to the power sector.

12.13. Feedback & Continuous Improvement: Update use cases, playbooks, and correlation rules based on newly discovered threats and lessons learned from previous incidents.

13. SECURITY INCIDENT ANALYSIS AND FORENSICS

13.1. The C-SOC shall implement a formalized incident analysis and digital forensics capability to ensure every security event is fully investigated, documented, and used to strengthen BESCOM's cyber resilience. The activities shall include, but not be limited to, the following:

13.2. Comprehensive Root Cause Analysis (RCA): Conduct in-depth RCA for all major and critical security incidents to identify the origin, attack vector, exploited vulnerabilities, and contributing process gaps.

13.3. Preservation of Evidence: Securely capture and preserve logs, memory dumps, network packet captures, and other relevant forensic artifacts in a tamper-proof and legally defensible manner, ensuring chain-of-custody documentation.

13.4. Malware & Payload Analysis: Analyze malicious files, binaries, or scripts using sandboxing and reverse-engineering techniques to understand capabilities, persistence mechanisms, and potential lateral movement.

13.5. Log & Artifact Correlation: Correlate data from SIEM, NBAD, DAM, firewalls, endpoint telemetry, and cloud logs to reconstruct attack timelines and identify patient-zero systems.

13.6. Incident Timeline & Impact Analysis: Produce a detailed timeline of attack progression, highlighting dwell time, initial intrusion, escalation, persistence, and exfiltration activities.

13.7. Post-Incident Reporting: Deliver comprehensive incident analysis reports containing technical findings, affected systems, root cause summary, business impact, and recommended corrective actions.

13.8. Lessons Learned & Control Enhancement: Conduct post-incident review meetings with stakeholders and update detection rules, security policies, and SOC playbooks to prevent recurrence of similar incidents.

13.9. Integration with Threat Intelligence: Feed newly discovered Indicators of Compromise (IOCs) and attacker techniques back into the TIP/SIEM for future detection and blocking.

13.10. Compliance with Evidence Retention Policies: Ensure logs and forensic artifacts are retained for the duration mandated by CERT-In, CEA Cybersecurity Guidelines 2021, and internal BESCOM policy.

13.11. Secure Evidence Repository: Maintain an encrypted, access-controlled evidence repository with strict audit logging of access and retrieval events

13.12. Post-Incident Reporting: Provide comprehensive post-incident reports, including the following:

a. Incident Details: Record the date, time, and location of the incident for accurate context.

b. Involved Parties: List individuals, witnesses, and their roles for responsibility tracking.

c. Timeline: Map out the sequence of events, from incident discovery to resolution, with specific times for each stage.

d. Incident Description: Provide a factual narrative outlining what happened before, during, and after the incident.

e. Immediate Actions: Note initial responses and emergency actions taken on the scene.

f. Impact Assessment: Evaluate the scale of consequences, such as harm to individuals, operational disruption, or data loss.

g. Root Cause Analysis: Analyze underlying reasons for the occurrence, such as process failures or human error.

h. Corrective Actions: Document and assign specific preventive measures to prevent recurrence.

i. Supporting Documentation: Attach relevant evidence like logs, screenshots, and photos.

j. Status and Review: Update report status (Draft, Reviewed, Closed) and share with stakeholders as it progresses.

14. Automation and Optimization

14.1. The C-SOC shall leverage automation, orchestration, and continuous optimization to maximize efficiency, reduce manual intervention, and improve the accuracy of detections and responses. The following activities shall be implemented:

14.2. SOAR Playbook Development & Deployment:

14.2.1. Design, configure, and deploy SOAR (Security Orchestration, Automation, and Response) playbooks for common use cases such as malware outbreak containment, phishing email takedown, user account lockouts, unauthorized login attempts, and suspicious network traffic.

14.2.2. Implement both semi-automated (human-in-the-loop) and fully automated workflows based on incident severity and predefined risk thresholds.

14.2.3. Continuous Use Case Optimization**:**Periodically review and fine-tune SOC use cases, SIEM correlation rules, and detection logic to improve true positive rates and reduce noise.Align all detection use cases with MITRE ATT&CK and NIST CSF frameworks to ensure comprehensive coverage of adversary tactics and techniques.

14.2.4. Dynamic Threat Intelligence Enrichment: Automate ingestion of threat intelligence feeds and real-time enrichment of alerts with IOCs, risk scores, and adversary context for faster triage.

14.2.5. Workflow Standardization: Document and standardize SOC workflows for incident detection, triage, escalation, and closure.Integrate these workflows with the ticketing system for full case lifecycle tracking and SLA compliance.

14.2.6. SOC Efficiency Metrics & KPIs:

a. Track key performance indicators such as automation coverage percentage, reduction in Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), false positive rate, and analyst workload reduction.

b. Report these metrics periodically to BESCOM management as evidence of SOC maturity improvement.

14.2.7. Scalability & Future-Proofing: Continuously optimize SOC architecture, storage, and processing capacity to handle increasing log volumes and new BESCOM applications as they are onboarded.

14.2.8. Version & Rule Management: Maintain version control for all correlation rules, playbooks, and automation scripts, with proper documentation of changes, approvals, and rollback procedures.

14.2.9. Integration Testing & Validation: Periodically test automated workflows and response actions in a controlled environment to validate effectiveness and ensure no unintended impact on production systems.

15. NTP server:

The Tenderer should configure NTP for the proposed solution to have uniform timestamps across BESCOM infrastructure/applications. The Tenderer should provide NTP server for each location (DC and DR) which in turn will relay the requests to NIC/external NTP server. The proposed NTP server should act as BESCOM's central NTP server and all the BESCOM's devices/services shall integrate with proposed NTP server. Accordingly, the sizing of the servers should be done.

16. Storage

The tenderer shall carry out storage sizing in accordance with the requirements and sizing specifications outlined in this tender document. However, the tenderer shall mandatorily provision a minimum storage capacity of 1500 GB per day, or the actual per-day storage requirement, whichever is higher, calculated based on the average volume of logs generated over a continuous one-month period after complete integration of all security tools and IT/OT/IoT applications in a period of subsequent 6 months.

All associated peripheral storage infrastructure, including but not limited to storage controllers, SAN switches, and related components, shall be supplied and configured in a High Availability (HA) architecture at the Data Center (DC), strictly as per the BoQ. The HA configuration shall be fully operational post complete integration of all tools and IT/OT/IoT applications. The vendor shall ensure automated, encrypted backups of all SIEM/SOC configurations, correlation rules, dashboards, and log indices within the organization's on-premise infrastructure. Backup cycles must follow a defined policy (daily incremental, weekly full) with

integrity validation and secure offline/DR copies retained as per regulatory requirements. Restoration procedures must be documented, tested quarterly, and support rapid recovery to ensure uninterrupted SOC operations.

17. Log retention: The proposed SIEM/SOC solution shall:

17.1. Store and process all logs fully On-Premise within the organization's Data center. Maintain minimum 180 days of hot (online) log retention and six months' log in archive compressed mode, extendable per regulatory mandates

17.2. Hot Storage (Online Log Storage)

The tenderer shall provision Hot Storage for real-time and near-real-time storage of security logs, events, alerts, flows, and telemetry data generated from all integrated IT, OT, and IoT systems on boarded to the SOC platform (SIEM/SOAR).

17.3. Logs shall include, but not be limited to:

a. Network devices (firewalls, routers, switches)
b. Servers, databases, applications
c. Endpoints, EDR/XDR
d. OT/SCADA, EMS, substations, PLCs
e. Cloud, SaaS, identity and access systems

17.4. Performance Requirements

Hot storage shall support real-time ingestion and analytics without data loss at peak EPS rates. The solution shall ensure:

- Low-latency search and correlation
- Real-time alerting and SOAR playbook execution
- Search queries for hot data shall return results within ≤ 5 seconds for standard SOC use cases.

17.5. Availability and Resilience

Hot storage infrastructure shall be deployed in High Availability (HA) mode with no single point of failure.

a. Minimum uptime shall be 99.9%.
b. Components including storage controllers, disks, and interconnects shall be redundant.

c. Hot storage shall be protected against disk failure, node failure, and data corruption.

17.6. Security and Compliance

a. Logs stored in hot storage shall be:
b. Encrypted at rest and in transit
c. Protected using role-based access control (RBAC)
d. Logged and audited for all access and administrative actions
e. Data integrity controls such as hashing/checksum validation shall be enabled.
f. Hot storage shall comply with:
g. CERT-In log retention directives
h. ISO/IEC 27001:2022 logging and monitoring controls
i. CEA cyber security guidelines for power sector

17.7. Sizing and Scalability

Hot storage sizing shall be based on:

a. Logs generated post complete integration of all identified log sources
b. Peak EPS, burst traffic, and future growth
c. The solution shall support horizontal and vertical scalability without service disruption.
d. Under-sizing of hot storage shall be treated as non-compliance.

17.8. Data Transition and Lifecycle Management

Logs shall be automatically transitioned from Hot Storage to Warm Storage and subsequently to Cold Storage as per defined retention policies.The transition process shall:

a. Preserve metadata, timestamps, and chain of custody
b. Be transparent to SOC operations

17.9. Audit and Verification

BESCOM or its authorized agency shall have the right to:

a. Verify hot storage capacity, performance, and retention
b. Conduct live search and alert validation tests
c. The tenderer shall support such audits at no additional cost.

17.10. Penalty Clause

Failure to maintain hot storage availability, performance, or retention shall attract penalties as per SLA. Repeated failures shall be treated as material breach of contract.

17.11. Warm Storage in Archive Mode for 6 months

The tenderer shall provision Warm Storage in Archive Mode for retention of security logs, alerts, events, and forensic artefacts generated from all integrated IT, OT, and IoT log sources connected to the SOC platform (SIEM/SOAR). Warm storage shall:

17.11.1. Retain logs in a compressed, indexed, and searchable format for a minimum period as specified in the tender.

17.11.2. Support near-real-time retrieval of archived logs for investigations, compliance audits, incident response, and regulatory requirements.

17.11.3. Ensure data integrity, immutability (WORM or equivalent), and protection against unauthorized modification or deletion.

17.11.4. Be seamlessly integrated with the SIEM/SOAR platform, enabling on-demand access without impacting production performance.

17.11.5. Include role-based access control, encryption at rest and in transit, and audit logging.

17.11.6. Be sized to accommodate logs generated post complete integration of all identified log sources, including peak log volumes.

17.12. Cold Storage for 1 Year

The tenderer shall provide Cold Storage for long-term retention of security logs, alerts, and incident data for a minimum period of one (1) year, in compliance with statutory, regulatory, and organizational requirements. Cold storage shall:

17.12.1. Retain logs in a non-indexed, cost-optimized archival format, with secure retrieval mechanisms.

17.12.2. Support secure retrieval within a defined SLA (to be specified by the tenderer) for audits, legal investigations, or post-incident analysis.

17.12.3. Ensure end-to-end encryption, data integrity checks, and tamper-proof retention.

17.12.4. Comply with applicable Government of India, sectoral, and regulatory guidelines related to log retention.

17.12.5. Be logically and physically segregated from production systems to prevent unauthorized access.

17.12.6. Be sized considering actual log volume generated after full SOC onboarding, including IT, OT, and IoT environments.

17.13. Ensure tamper-proof, encrypted retention with audit trails and cryptographic integrity checks

17.14. Support rapid indexing/search & retrieval to aid investigation and compliance response

17.15. Enforce time synchronization across all log sources for accurate correlation

17.16. Offer redundancy & DR within organization premises with 99.9% data availability

17.17. Support policy-based lifecycle management for archived data.

17.18. Tenderer shall submit:

- Retention Architecture
- Regulatory Compliance Mapping (CERT-In / RBI / SEBI)
- Annual integrity and retention conformance report

18. Integration Requirements:

18.1. The proposed solution must ensure seamless on-premise integration with: Security Detection & Response Controls:

Technology	Required Focus
SOAR	Automated response, workflow orchestration & ITSM linkage
UEBA	Identity and behavior anomaly detection
NBAD	Network deviation & lateral movement detection
EDR	Endpoint telemetry, incident enrichment, host containment
Others	Other tools and technologies as per BoQ

18.2. **Platform Capabilities:**

a. Ingestion via Syslog, API, Web hooks, Agent/Agentless methods
b. Deep correlation across identity, network, endpoint & cloud events
c. Prebuilt MITRE ATT&CK mapped use case libraries
d. Ability to onboard new log sources without OEM dependency
e. Full integration services provided by the tenderer

18.3. **Tenderer shall submit:**

a. Integration Runbook
b. Log Source Coverage Matrix
c. Support timelines & accountability for ongoing onboarding

18.4. **Solution Integration, Commissioning, and Go-Live**

a. End-to-End Solution Integration: The tenderer shall deploy and integrate all security solutions including SIEM, SOAR, TIP, NBAD, DAM, WAF, EDR, DLP, RASP and DDoS protection with BESCOM's IT, OT, IoT, and Cloud infrastructure.
b. Functional and Stress Testing: The tenderer shall perform rigorous integration, performance, and failover testing to verify that deployed solutions handle live production workloads without disruption.
c. Simulated Attack Drills: The tenderer shall conduct controlled red-team/blue-team exercises and mock cyberattack simulations to validate SOC detection and response readiness before go-live.
d. Formal Commissioning: The tenderer shall submit detailed go-live reports including baseline health metrics, coverage matrix, and system performance statistics, followed by BESCOM's formal sign-off within six months (implementation phase).

19. BESCOM Dashboards & Reporting Requirements

The proposed solution shall:

19.1. Provide CISO-level and Management dashboards with real-time risk scoring & threat landscape view

19.2. Include operational KPIs: MTTD, MTTR, MTTE, FPR, SLA compliance

19.3. Offer Automated reporting cadence:

19.4. Provide export in PDF, PPT, Excel formats

19.5. Support role-based access & customization without vendor intervention

20. Threat Modelling & Use Case Requirements:

The proposed detection framework shall:

20.1. Implement threat modelling aligned to MITRE ATT&CK, NIST CSF & Zero Trust

20.2. Cover high-risk scenarios.

20.3. Provide threat hunting playbooks & predefined containment actions.

20.4. Ensure quarterly tuning and enhancement with CISO approval.

20.5. On-Premise Deployment Compliance.

20.6. The entire SIEM/SOC solution including log storage, analytics, dashboards, and SOAR must be hosted and processed fully On-Premise

20.7. No data transmission, analytics, or storage outside organizational control is allowed

20.8. Vendor must certify Data Privacy, Residency & Sovereignty compliance

20.9. Provide scalable On-Prem architecture plan for growth requirements.

21. Standards Compliance and Security Governance:

The tenderer shall ensure that the SOC design, deployed technologies, and operational processes comply with Global Standards Alignment as below but not limited to:

a) ISO/IEC 27001:2022 – Information Security Management System (ISMS)
b) ISO 22301:2019 – Business Continuity Management System (BCMS)
c) IEC 62443 – Cybersecurity for Industrial Automation and Control Systems
d) ISO/IEC 27035 – Incident Management
e) ISO/IEC/IEEE 24748-1: 2018 Systems and Software Engineering – Life Cycle Management – Part 1: Guidelines for life cycle management.
f) ISO/IEC/IEEE 15288 and 2207 – Life cycle management of systems and software – system engineering processes.
g) NIST SP800 -160 Vol 1 - Engineering Trustworthy Secure Systems (adds security engineering specialty domain aspects to systems engineering defined in ISO 15288).
h) ISO/IEC 42010:2011 – Systems and Software Engineering – Architecture description.

Other relevant ISO/IEC, NIST CSF, and BIS standards applicable to BESCOM's IT/OT/IoT environments

22. Tenderer/OEM Audit:

22.1. The Tenderer shall conduct an annual audit of the deployed SIEM/SOC platform to validate performance, configuration, and security compliance.

22.2. Audit must verify log retention, integrity controls, correlation accuracy, and adherence to regulatory mandates.

22.3. OEM shall review use cases, enrichment pipelines, and threat detection efficacy against MITRE ATT&CK.

22.4. Findings must include gaps, optimisation recommendations, and roadmap enhancements.

22.5. OEM shall certify that all components remain compliant with on-premise deployment and data sovereignty requirements.

22.6. A formal audit report must be submitted to the CISO with corrective actions and implementation timelines.

23. Training:

23.1. **Structured Training Programs:** The tenderer shall deliver comprehensive, role-based training covering SOC operations, SIEM dashboards, SOAR playbooks, log analysis techniques, threat hunting, incident triage, and escalation procedures.

23.2. **Tabletop and Hands-on Exercises:** The tenderer shall conduct periodic incident simulation drills (phishing, ransomware, insider threat, DDoS, OT compromise) to build response maturity and improve Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).

23.3. **Technical Documentation Handover:** The tenderer shall provide detailed architecture diagrams, configuration baselines, standard operating procedures (SOPs), use case catalogs, and incident playbooks for BESCOM's internal use.

23.4. **Knowledge Transfer Workshops:** The tenderer shall facilitate interactive sessions for BESCOM teams covering:

a) Vulnerability management lifecycle and risk-based prioritization
b) Threat intelligence interpretation and operationalization

c) Digital forensics and evidence preservation procedures
d) Compliance reporting, audit readiness, and regulatory engagement

23.5. **Skill Development Recommendations:** The tenderer shall suggest relevant certifications and training pathways (SOC Analyst, Incident Handler, Threat Hunter, Forensic Analyst) to help BESCOM build a skilled in-house security workforce.

23.6. **Post-Go-Live Mentorship:** Provide handholding support for a defined stabilization period to ensure BESCOM teams can independently operate, monitor, and maintain SOC functions effectively.

24. Severity & Escalation Matrix:

24.1. ISO/IEC 27035 is an international standard that provides guidelines for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an effective information security incident management system. It is part of the ISO/IEC 27000 family of standards and focuses on the lifecycle of security incidents, including preparation, detection, assessment, response, and lessons learned.

24.2. **The standard emphasizes:**

a) Structured Incident Handling: Ensuring incidents are identified, classified, and managed systematically.

b) Risk-Based Prioritization: Classifying incidents based on impact and urgency to allocate appropriate response resources.

c) Defined Roles and Responsibilities: Establishing accountability across IT, security, and business units.

d) Continuous Improvement: Learning from incidents to enhance security controls, policies, and operational procedures.

e) Provides a globally recognized framework for SOC incident management.

f) Guides incident severity classification and response prioritization.

g) Establishes escalation procedures, ensuring the right stakeholders are informed at the right time.

h) Supports integration with SIEM, SOAR, TIP, and EDR tools for automated and efficient response.

i) Enables continuous improvement of SOC processes, dashboards, and playbooks.

24.3. **Need for Incident Severity and Escalation Matrices in SOC**:

24.3.1. **A Cyber Security Operations Center (SOC)** must respond to threats promptly and efficiently to minimize damage to critical IT, OT, IoT, and cloud systems. **Incident Severity Matrices** and **Escalation Matrices** are essential for this purpose:

a) <u>Incident Severity Matrix:</u>

I. Categorizes security events based on **impact on business operations and urgency of response**.
II. Enables SOC teams to **prioritize critical threats** like ransomware, data breaches, or OT anomalies over less impactful events.
III. Ensures consistency in classification, aligning with international standards like ISO/IEC 27035, NIST SP 800-61, and ITIL 4.

<u>Incident Severity Matrix – Standard Mapped</u>

Severity	**Description**	**Impact on BESCOM**	**Response Time (SLA)**	**Resolution Target (SLA)**	**Mapped Standards**
Critical (P1)	Active cyberattack (ransomware, data breach, SCADA compromise) or major system outage affecting critical IT/OT/IoT/Cloud services	Complete disruption of business-critical services; regulatory or statutory impact; high reputational risk	15 minutes (ISO 27035, NIST)	≤ 4 hours (CERT-In)	ISO/IEC 27035, NIST SP 800-61, CERT-In
High (P2)	Malware outbreak, phishing attack, insider threat, or threat with significant potential impact	Partial service disruption; moderate regulatory/compliance risk	30 minutes	≤ 8 hours	ISO/IEC 27035, NIST,

Severity	Description	Impact on BESCOM	Response Time (SLA)	Resolution Target (SLA)	Mapped Standards
Medium (P3)	Policy violations, suspicious but non-critical alerts, minor vulnerability detected	Limited operational impact; no critical service downtime	1 hour	≤ 24 hours	ISO/IEC 27035,
Low (P4)	Informational alerts, minor anomalies, non-critical events	Minimal impact, no disruption	4 hours	≤ 3 business days	ISO/IEC 27035,

b) <u>Escalation Matrix</u>

I. Defines **tiered escalation paths** for different severity levels, ensuring incidents reach the right personnel promptly.

II. Facilitates timely **decision-making, coordination, and communication** during high-impact events.

III. Supports regulatory and compliance obligations, including CERT-In reporting for critical incidents.

24.3.2. Together, these matrices provide a structured, auditable framework for SOC operations, ensuring rapid detection, timely response, and effective resolution of security incidents while maintaining compliance with global best practices and standards.

Escalation Matrix – Standard Mapped

Severity	SOC Analyst / Level 1	SOC Team Lead / Level 2	SOC Manager / Level 3	BESCOM ISMS / Senior Officials	Mapped Standards
P1 – Critical	Immediate detection & initial response	Within 15 minutes	Within 30 minutes	Within 1 hour; notify CISO / GM	ISO 27035, NIST, CERT-In
P2 – High	Immediate triage	Within 30 minutes	Within 1 hour	Within 2 hours; notify SOC Manager & ISMS	ISO 27035, NIST,

Severity	SOC Analyst / Level 1	SOC Team Lead / Level 2	SOC Manager / Level 3	BESCOM ISMS / Senior Officials	Mapped Standards
P3 – Medium	Logged and triaged	Within 1 hour	Within 4 hours	Escalate if unresolved > 24 hours	ISO 27035,
P4 – Low	Logged in ticketing system	Within 4 hours	Review in daily report	Escalate if unresolved > 3 business days	ISO 27035,

25. SOC Dashboard Design and Implementation

25.1. Objective:

25.1.1. The objective of the SOC dashboard is to establish a unified, centralized, real-time monitoring and visualization platform for BESCOM's Cyber Security Operations Centre (C-SOC). The dashboard shall serve as a single source of truth for security operations, incident management, compliance tracking, and executive decision-making.

25.1.2. It shall provide role-based visibility to stakeholders including SOC Analysts, SOC Managers, CISO, IT Heads, and BESCOM Leadership, enabling them to take informed decisions based on timely, accurate, and actionable security intelligence.

25.1.3. Separate dash board shall be designed and provided for IT, OT and IoT applications.

25.1.4. The selected tenderer shall design, develop, configure, implement, and hand over a fully functional SOC Dashboard, which:

a) Integrates with all tools and platforms deployed under BESCOM C-SOC (SIEM, SOAR, TIP, UEBA, NBAD, DAM, EDR, Vulnerability Management, Patch Management, and Threat Intelligence).

b) Consolidates log data, alerts, events, vulnerabilities, threat indicators, user anomalies, and operational KPIs into meaningful, contextual visualizations.

c) Provides end-to-end visibility into security posture across IT, OT, and IoT applications, systems, and networks.

d) Is capable of supporting multi-tenant and multi-layer views, ensuring segregation of data and compliance with regulatory requirements.

25.1.5. **Incident & Threat Intelligence View:**

a) Real-time display of incident severity breakdown (Critical, High, Medium, Low).

b) Drill-down capability from high-level KPI to incident details, log source, and forensic data.

c) Integration with Threat Intelligence Feeds (global & national sources such as CERT-In, NCIIPC, ISACs).

d) Display of IOC sightings, malware campaigns, and attack techniques (mapped to MITRE ATT&CK framework).

25.1.6. **Performance & SLA Monitoring**

a) Metrics for MTTD (Mean Time to Detect), MTTR (Mean Time to Respond), MTTC (Containment).

b) Real-time display of SOC SLA compliance, incident closure rates, and backlog analysis.

c) Automated SLA violation alerts and escalation triggers per the defined Escalation Matrix.

d) Customization & Flexibility:

I. Drag-and-drop widget-based interface with ability to create and save custom dashboards.

II. Multi-level filters (time range, incident type, severity, asset group, department).

III. Ability to generate printable PDF/Excel reports from dashboard views.

IV. Multi-language support (English + local language if required).

25.1.7. **Security & Compliance Requirements**

a) The dashboard shall be hosted within BESCOM premises with no data leaving the BESCOM network.

b) All communication shall be encrypted using TLS 1.3 or higher**.**

c) Dashboard access must be controlled through MFA-enabled RBAC (Role-Based Access Control) integrated with BESCOM AD/SSO.

d) All user activities (logins, view changes, configuration edits) must be logged and auditable for at least 1 year**.**

e) Solution must comply with ISO/IEC 27001:2022**,** CERT-In guidelines, and sectoral cyber security advisories.

25.1.8. **User Experience & Design Principles**

a) Intuitive, minimalistic UI/UX optimized for quick decision-making.

b) Color-coded severity levels mapped to BESCOM's Incident Severity Matrix.

c) Responsive design for viewing on desktops, large screens in SOC NOC Room, and tablets.

d) Capability to project on a Video Wall in the SOC for 24×7 monitoring.

e) Adherence to accessibility guidelines (WCAG 2.1) for visually impaired staff if required.

25.1.9. **Dashboard Templates (Minimum) :** The tenderer must deliver the following pre-designed dashboards at Go-Live:

a) Executive Dashboard:

I. High-level KPIs, risk trends, compliance scores, SLA adherence

II. Intended for CISO, CXOs, BESCOM Board members

b) Operational Dashboard:

I. Real-time incidents, alerts, event correlation, analyst work queue

II. Designed for SOC Analysts and L1/L2 teams

c) Compliance Dashboard:

I. ISO 27001 control coverage, CERT-In reporting status, vulnerability closure rates

II. For internal audit, regulators, and compliance team

26. Documentation for the solution:

26.1. **Documentation for hardware and software components:** The Tenderer shall deliver all the relevant documents to BESCOM for all hardware and software components including third party software before the "Cyber Security Operations Centre, (C-SOC) and other security solutions at BESCOM" becomes operational, which may include, but not limited to software licenses certificate, user manuals, installation manuals, operation manuals, design documents, process documents, technical manuals, functional specification, on-line tutorials, system configuration documents, system administrative documents, debugging/diagnostics documents, test procedures etc.

26.2. **Documentation for the solution:** Tenderer shall deliver all relevant documentation pertaining to entire solution in the appropriate format. The indicative list may include but not limited to-

26.2.1. **Project Plan:** The tenderer should provide a detailed project plan as per the delivery schedule (Section 4.1.2). The project plan should detail the tasks that will be carried out and completed on various scheduled dates including acceptance testing. The project plan shall become final when it has been accepted by BESCOM. The tenderer shall submit weekly report on progress of the project and also the status as on the scheduled date and actual date of each activity.

26.2.2. Design document: The design document should include (but not limited to) solution architecture, low level design details, technology/solution wise detailed architecture, etc. The Design document shall become final when it is accepted by BESCOM

26.2.3. **During Delivery stage:**

a) Proof of delivery of the components (hardware & software licenses)
b) Submission of delivery challan
c) Proof of latest version of hardware and software

d) Information related to End of Life & End of Support of all components of NGSOC project
e) Proof of Licenses (hardware and software) with validity
f) Inventory list for "Next Generation Security Operations Centre, Network Operations Centre (NGSOC) and other security solutions at BESCOM" project.
g) Back to back OEM support certificate

26.2.4. **During implementation stage**

a) Installation Document
b) Configuration and integration document, installation manual, operational and user manual
c) Project Management Reports (On weekly basis commencing from the date of signing the contract) – Project Status Reports
d) UAT Test Plans
e) SOP documents including (but not limited to) operational, troubleshooting, analysis SOPs for all the solutions proposed as part of this project.
f) BCP-DR plan including RTO and RPO testing report in compliance with requirement of RFP.
g) Risks and Mitigation Document
h) Operational Acceptance Checklist
i) Operation Manuals
j) Any other technical manuals required for the operation of any of the components.
k) Hardening documents for each solution component
l) VAPT compliance report, VAPT corrective actions and resolution report
m) Develop Standard Operating Procedures (SOPs) for monitoring, escalation, incident response, and reporting.
n) Conduct workshops and training for BESCOM personnel on SOC tools, dashboards, and processes.
o) Deliver comprehensive documentation, including architecture diagrams, configuration baselines, and integration details.

26.2.5. **Deliverables:**

a) **Detailed Design Document** with data flow diagrams, integration points, and security controls.

b) **SOPs and Admin Manuals** for managing and customizing dashboards.

c) **User Training & Knowledge Transfer** sessions for SOC staff and BESCOM IT team.

d) **Test Reports** for load, performance, and failover scenarios.

27. CSOC Acceptance Criteria:

The dashboard will be considered accepted upon successful completion of:

27.1. **Integration Testing:** Verification that all log sources, alerts, and KPIs are accurately displayed.

27.2. **UAT (User Acceptance Testing):** Sign-off from BESCOM Security Team and Stakeholders.

27.3. **Performance Testing:** Demonstration of ≥ 99.9% availability and ≤ 3-second response time under peak load.

27.4. **Knowledge Transfer Completion:** Confirmation of at least two sessions for operations and customization training.

27.5. All FAT, SAT, and UAT activities shall be witnessed and signed-off by **BESCOM's ISMS/SOC Governance Committee**.

27.6. The tenderer shall provision all test data, attack simulation tools, and resources required for testing.

27.7. **Defect Resolution Policy:** All Critical/Major defects must be closed before UAT sign-off; BESCOM reserves the right to demand re-testing at no additional cost.

27.8. **Final Acceptance:** Shall be granted only after successful UAT, closure of all observations, and stabilization period agreed with BESCOM.

27.9. **Testing and Go-Live :** Conduct end-to-end functional, integration, and failover testing.

27.10. Execute Red Team / Blue Team simulations to validate detection and response capabilities.

27.11. Commission the C-SOC officially into production upon BESCOM sign-off.

27.12. **Shared Billing Infrastructure Security**

1. Integrate logs from multiple ESCOM's infrastructure components with defined classification & segregation.

Implement strict segregation of access, ensuring BESCOM systems are isolated from other ESCOM IP ranges.

2. Maintain comprehensive tamper-evident audit logs for all shared billing system activities.

3. Ensure compliance with ISO/IEC 27001, CERT-In guidelines, and regulatory requirements. Enforce access control with MFA, RBAC, firewall policies, VLAN segregation, and continuous monitoring.

4. The Tenderer shall provide technical assurance and a formal undertaking to implement these measures before SOC commissioning.

27.13. **FAT, SAT, and UAT Clauses for SOC Setup:**

27.13.1. Factory Acceptance Test (FAT) - Objective

The purpose of the FAT is to validate that all proposed SOC infrastructure components, software modules, and integrations strictly conform to the approved Bill of Material (BoM), High-Level Design (HLD), Low-Level Design (LLD), and Technical Specifications before shipment and deployment at BESCOM premises.

27.13.2. FAT Scope:

The successful tenderer shall perform FAT at the OEM premises or the System Integrator's staging lab in the presence of BESCOM's designated evaluation committee. FAT shall comprehensively cover:

i. **Hardware Validation**

a) Verification of servers, storage appliances, network switches, firewalls, HSMs, and security devices.

b) Compliance with capacity, EPS throughput, redundancy, and performance benchmarks specified in the RFP.

ii. **Software & Licensing Validation**

a) Confirmation that all software modules (SIEM, SOAR, TIP, EDR, DAM, NBAD, VM, RASP, ESAM,

UEM, IAM, WAF, DDoS Protection) are available in correct versions and licensed per agreed quantities.

iii. **Integration Readiness**

a) Verification of APIs, connectors, and log parser packs for all BESCOM applications, IoT/OT systems, and network devices.

b) Validation of baseline integrations and log flow in the lab environment.

c) Log sources shall be integrated through dedicated and logically segregated VLANs to ensure secure, scalable, and interference-free onboarding to the SIEM/SOAR platform. Granular firewall rules shall be implemented to enforce strictly unidirectional data flow (one-way traffic) using allow-list–based policies. For OT system integration, hardware- or software-based data diode solutions shall be provisioned to ensure deterministic one-way communication from OT to IT/SIEM environments, thereby preventing any inbound access, command execution, or lateral movement into the OT network.

iv. **Baseline Configuration**

a) Installation of default correlation rules, SOAR playbooks, dashboards, reports, and compliance templates.

b) Security hardening as per **CIS Benchmarks** or OEM best practices.

v. **Documentation Review**

a) Submission and validation of HLD/LLD, network diagrams, SOPs, BoQ mapping, and security configuration documents.

27.13.3. **FAT Deliverables**

I. **FAT Test Plan** (approved by BESCOM prior to execution).

II. **FAT Test Report** including detailed results, screenshots, and observations.

III. Closure of all FAT findings with corrective actions prior to shipment.

IV. **Acceptance Criteria:** Shipment to BESCOM is permitted **only after formal FAT sign-off** by BESCOM's authorized representatives.

27.13.4. Site Acceptance Test (SAT)

27.13.4.1. **Objective:**

SAT validates that all SOC components are correctly **installed, integrated, configured, and fully functional** in BESCOM's production environment and meet performance, resiliency, and security requirements.

27.13.4.2. **SAT Scope:**

a) **Infrastructure Validation:** Verification of racks, power availability, structured cabling, network connectivity, and redundancy.Validation of system health, clustering, and HA/failover capabilities.

b) **Tool-Wise Functional Validation**

Tool / Component	**Key SAT Validation Activities**
SIEM	Log onboarding from representative sources, parser validation, correlation rule triggers, storage retention verification.
SOAR	End-to-end playbook execution (malware isolation, IP block), ticket creation, approval and closure workflows.
TIP	Threat feed ingestion, IOC enrichment, and correlation with SIEM alerts.
EDR	Agent deployment, detection of controlled malware sample, isolation and rollback verification.
DAM	Database audit log capture, policy enforcement, and alert testing.
NBAD/UEBA	Baseline profiling validation, anomalous network/user behavior detection.
VM	Vulnerability scans execution, prioritization, and report export validation.
RASP	Runtime attack detection, payload blocking, and event logging verification.

Tool / Component	Key SAT Validation Activities
ESAM	Continuously identify, monitor, and reduce vulnerabilities within an organization's internet-facing assets, such as web servers, cloud services, APIs, domains, and shadow IT resources.
UEM	Endpoint compliance enforcement (patch check, USB control, posture compliance).
IAM	MFA, SSO integration, and RBAC enforcement validation.
WAF	Blocking of OWASP Top-10 attack payloads, tuning for false positives.
DDoS Protection	Simulation of volumetric traffic, ensuring service continuity under attack.

27.13.4.3. **Performance & Resiliency Validation**

a) Validation of SIEM EPS handling capacity under peak load.

b) Dashboard refresh rate (<3 seconds), alert latency, and SOAR response time.

c) Failover, DR switchover, and HA testing for mission-critical components.

27.13.4.4. **SAT Deliverables**

a) Approved SAT Plan & Checklist (prior to execution).

b) SAT Test Report including logs, screenshots, and detailed observations.

c) List of deviations with RCA and agreed resolution timelines.

27.13.4.5. Acceptance Criteria: SAT is deemed successful only after all critical issues are resolved and BESCOM provides formal SAT sign-off.

27.13.5. **User Acceptance Testing (UAT)**

27.13.5.1. Objective: UAT ensures that the SOC platform delivers the expected business outcomes, compliance posture,

and operational workflows and that BESCOM's SOC team is capable of operating the solution effectively.

27.13.5.2. UAT Scope:

a) End-to-End Incident Validation
   I. Simulated scenarios: phishing, insider threat, ransomware outbreak, DDoS attack.
   II. Full chain validation: Detection → Alert → Investigation → Automated Response → RCA Report.

b) Dashboard & Reporting Verification:
   I. Validation of SLA/KPI dashboards (MTTD, MTTR, dwell time), heatmaps, compliance views.
   II. Export of reports (PDF, CSV) and generation of regulatory reports (CERT-In, ISO 27001).

c) Escalation & SLA Workflow Testing: Incident severity matrix validation, SLA breach alerts, escalation notifications to management.

d) Knowledge Transfer Validation:
   I. Practical hands-on evaluation of SOC staff post-training.
   II. Review and acceptance of SOPs, playbooks, and runbooks.

27.13.5.3. UAT Deliverables:

a) UAT Plan & Scenario Matrix approved by BESCOM.
b) UAT Report with pass/fail results, screenshots, and findings.
c) Training Completion & Knowledge Transfer sign-off.
d) Acceptance Criteria: UAT sign-off confirms Go-Live readiness. Any open items must have documented mitigation plans and agreed resolution timelines before cut-over

28. Warranty and Support Phase

28.1. Operation and maintenance of all deployed security solutions throughout the contract period.
28.2. Five-year onsite comprehensive warranty covering installation, reinstallation, and configuration without additional cost.
28.3. Provision of version upgrades, patches, program updates, critical security alerts, and documentation updates.
28.4. 24x7x365 support for security solution malfunctions, with online request logging.
28.5. Immediate resolution of performance issues, bugs, and errors, including customizations, interfaces, and integration components.

28.6. Version control, change management, and impact assessment for all software upgrades and modifications.
28.7. Deployment of qualified personnel for SOC operations with prior background verification and continuous presence at BESCOM.
28.8. Coordination with other system integrators to ensure smooth operations without disruption.
28.9. Reports (daily, weekly, monthly, quarterly) in agreed formats approved by BESCOM ISMS.
28.10. Continuous monitoring and alerting for loss of log data, functional issues, or system malfunctions.

29. Governance & Change Control:

29.1. Any new dashboard widget, data source, or KPI introduced during the contract period must follow the Change Request (CR) process defined in the GCC/SCC and be approved by BESCOM ISMS Committee before deployment in production.

29.2. **Change Request (CR) Management:**

29.2.1. **Objective:**

To establish a formalized, structured, and auditable framework for managing any modifications, enhancements, upgrades, or adjustments to the C-SOC infrastructure, applications, processes, tools, and services during the contract period. This framework shall ensure that all changes are executed with minimal operational disruption, full accountability, and compliance with BESCOM's Information Security Management System (ISMS) policies, contractual Service Level Agreements (SLAs), and applicable regulatory requirements.

29.2.2. **Scope & Responsibilities:**

29.2.2.1. Change Request Initiation: All proposed changes shall be submitted through a standardized CR template, clearly specifying:

a) Detailed scope and objective of the change
b) Technical and operational impact analysis
c) Cybersecurity and regulatory implications
d) Required resources (human, technical, and financial)
e) Proposed timelines for implementation
f) Estimated costs (if applicable)
g) CRs may be initiated by BESCOM or the vendor but require formal logging in the CR register.

29.2.2.2. Impact Assessment: Vendor shall perform a comprehensive assessment of each CR, covering:

a) Operational impact including downtime, service availability, and dependencies
b) Cybersecurity risks and potential vulnerabilities introduced
c) Compliance implications under statutory, regulatory, and contractual obligations
d) Interdependencies with ongoing or scheduled activities within C-SOC
e) Assessment outcomes must be documented and submitted along with mitigation strategies.

29.2.2.3. Approval & Authorization:

a) All CRs shall undergo formal approval by the BESCOM ISMS/Change Advisory Board (CAB) before execution.
b) No change shall be implemented without written authorization.
c) Emergency changes (critical patches or security fixes) must follow an expedited approval workflow while still being documented and auditable.

29.2.2.4. Implementation Control:

a) Vendor shall ensure controlled deployment, including:
b) Pre-deployment backup and configuration snapshots
c) Testing in a staging or isolated environment (where feasible)
d) Rollback and recovery procedures clearly defined and tested
e) Verification and validation of successful implementation

29.2.2.5. Documentation & Knowledge Updates:

8.4.1.1.1 All related documentation, SOPs, dashboards, playbooks, and knowledge bases shall be updated post-CR.

8.4.1.1.2 CR closure must include lessons learned and operational notes.

8.4.1.1.3 Communication & Notification:

8.4.1.1.4 Schedule, expected downtime, and operational impact shall be communicated to all relevant BESCOM stakeholders in advance.

8.4.1.1.5 Vendor shall maintain clear logs for all communications.

29.3. Reporting & Audit:

29.3.1. Vendor shall maintain a monthly CR log including all submitted, approved, rejected, and implemented changes.

29.3.2. Logs shall be auditable and made available to BESCOM on demand.

30. Exit Management

30.1. Objective:

To ensure a secure, orderly, and fully auditable transition of C-SOC operations, systems, data, knowledge, and tools to BESCOM or its nominated successor without any disruption to operations or compromise of security.

During the contract period – If the contractor wishes to take exit from the contract, 6 months' prior notice to be given to the employer. The contractor shall carry out the following activities to complete exit formalities:

- Functional & Technical knowledge transfer of tools and technologies of all C-SOC apps to the personnel identified by BESCOM.
- Execute all the documents that may be necessary to effectively transfer the ownership and title, including OEM warranties in respect of all equipment's/software etc.,
- All related documentation and other configurable items etc., if any, in Contractors possession.
- List of all IT assets, subscription details, crenditals, passwords etc., at all locations to BESCOM.
- In the event of termination or expiry of the Contract, both the Contractor and BESCOM shall comply with the provision of Exit plan. During the exit management period, the Contractor uses its best efforts to continue delivery of all regular services. In addition, the successful tenderer shall ensure that complete handover of the processes, products, software licenses, tools, source codes, reports, documents, manuals, data, web content and other intellectual property rights to BESCOM.

During the contract period – If the BESCOM wishes to withdraw the contract, 3 months of prior notice will be given to the contractor. The contractor shall carry out following activities to complete exit formalities:

- Functional & Technical knowledge transfer of tools and technologies of all C-SOC apps to the personnel identified by BESCOM.
- Execute all the documents that may be necessary to effectively transfer the ownership and title, including OEM warranties in respect of all equipment's/software etc.,
- All related documentation and other configurable items etc., if any, in his possession.
- List of all IT assets, subscription details, crenditals, passwords etc., at all locations to BESCOM.
- In the event of termination or expiry of the Contract, both the successful tenderer and BESCOM shall comply with the provision

of Exit plan. During the exit management period, the successful tenderer uses its best efforts to continue delivery of all regular services. In addition, the Contractor shall ensure that complete handover of the processes, products, software licenses, source codes, reports, documents, manuals, data, web content and other intellectual property rights to BESCOM.

After the contract period the contractor shall will carry out following activities to complete exit formalities:

- Functional & Technical knowledge transfer of tools and technologies of all C-SOC apps to the personnel identified by BESCOM.
- Execute all the documents that may be necessary to effectively transfer the ownership and title, including OEM warranties in respect of all equipment's/software etc.,
- All related documentation and other configurable items etc., if any, in his possession.
- List of all IT assets, subscription details, crenditals, passwords etc., at all locations to BESCOM
- In the event of termination or expiry of the Contract, both the Contractor and BESCOM shall comply with the provision of Exit plan. During the exit management period, the Contractor uses its best efforts to continue delivery of all regular services. In addition, the contractor shall ensure that complete handover of the processes, products, software licenses, source codes, reports, documents, manuals, data, web content and other intellectual property rights to BESCOM.
- As part of the exit management process, the contractor shall obtain a written undertaking from all personnel involved in the project, affirming that they will not disclose, share, or misuse any confidential information or project-related data obtained during their engagement, even after the termination of their assignment.

30.2. Scope & Responsibilities of the Tenderer:

30.2.1. **Knowledge Transfer:**

a) Comprehensive sessions covering architecture, operational workflows, SOPs, dashboards, playbooks, monitoring and alerting procedures.

b) Detailed demonstration of system configurations, integration points, custom scripts, automation modules, and SIEM/SOAR rules.

30.2.2. **Data & Documentation Handover:**

a) Transfer of all operational data, logs, audit trails, incident reports, reports, scripts, parsers, and automation modules.

b) Delivery of up-to-date, verified documentation including SOPs, CR logs, change impact reports, and security configurations.

30.2.3. **Tools, Licenses & Access:**

a) Handover of all software licenses, administrative credentials, access rights, hardware, and configurations.

b) Secure decommissioning or handover of hardware/software as applicable.

30.2.4. **Pending Activities:**

a) Resolution of all open incidents, CRs, vulnerabilities, and compliance reports.

b) Handover of monitoring and alerting responsibilities to BESCOM or its successor.

30.2.5. **Transitional Support:**

Vendor to provide defined transitional support for a period of 30–60 days**,** including on-call assistance, knowledge clarification, and issue resolution.

30.2.6. **Compliance & Audit:**

Exit process shall be fully documented, auditable, and compliant with statutory, regulatory, and ISO/IEC 27001 cybersecurity standards.

31. EDR Deployment, Licensing and SIEM/SOAR Integration

The project envisages an indicative total of 6,000 EDR endpoints, comprising 5,000 currently identified endpoints and 1,000 additional endpoints anticipated over the next five (5) years. This quantity is indicative and intended solely for evaluation purposes. Payments shall be made strictly on a per-agent, per-year basis, based on the actual number of EDR agents deployed, licensed, and/or integrated with SIEM and SOAR. No lump-sum payments shall be considered, irrespective of the estimated quantity.

Successful Tenderers shall provide separate unit prices per endpoint per year for:

1. EDR Deployment and Licensing, and
2. EDR Integration with SIEM and SOAR.

The EDR Deployment and Licensing unit price shall be inclusive of agent deployment and configuration, license subscription, server connectivity,

updates, upgrades, patches, and OEM support. The SIEM/SOAR integration unit price shall include log ingestion and normalization, correlation and use-case mapping, alert analysis and tuning, and SOAR playbook integration with incident response support.

BESCOM presently has 1,303 EDR-enabled endpoints under an existing contract. For these endpoints, tenderers shall quote unit prices per agent per year exclusively for SIEM and SOAR integration. No EDR deployment or licensing charges shall be payable for these endpoints until the expiry of the existing EDR contract, and payments during this period shall be restricted solely to integration and analysis services.

Upon completion of one (1) year from the date of implementation, and only after expiry of the existing EDR contract, the 1,303 endpoints shall be on boarded to the selected tenderer's EDR solution. For the remaining years of the CSOC project/contract period or after expiry of the existing EDR contract, the C-SOC tenderer shall provide EDR deployment (if required), licensing, and full SIEM/SOAR integration.

BESCOM reserves the right to increase or decrease the number of endpoints during the contract period. Payments shall be limited strictly to the actual number of EDR agents deployed and/or integrated per year, and no charges beyond the quoted unit prices shall be admissible.

32. Requirements:

Secure architecture deployment for OT SOC with complete security controls in place as per the CIS level 2 benchmarks or in line with STIG framework.

Proper encryption mechanism may be provided in respect of log data being collected from various sites.

1. Next Generation SIEM /SOC shall have following features

   (a) Robotic/ Beaconing based threat detection.

   (b) DGA based threat detections.

   (c) Device Agnostic i.e. capable of ingesting logs of devices with different make, model, log format and functionality across the ICT infrastructure with built-in parsers.

   (d) Enrichment capabilities like geo-ip, threat attributes, asset tagging, whitelisting etc.

2. The following functionalities should be configured on the CSOC dashboard for enhancing the efficiency of CSOC:

   (a) Risk manager component to be added/activated in SIEM for generating alert for vulnerabilities in software /Applications/Firmware used in the entire IT stack through updated SBOMs (Software Bill of Materials).

   (b) Monitoring of privileged user/ administrator and important user accounts with regards to successful, failed logins and off-time logins. Generate alerts for anomalies.

(c) Monitoring of successful logins to user accounts beyond office working hours and generate alerts for accounts from which this activity is observed beyond a pre-defined threshold (recommended value 10).

(d) Monitoring and alert for repeated lockouts and authentication failure attempts across entire OT/SACDA and their host IT machines.

(e) Monitoring of external connections to sites/ destinations that are denied as per the security policy of Network. Generate alerts when any OT asset in the network crosses the predefined threshold (recommended value 10).

(f) Suitable alerts should be configured for timely detection of successful/ failed logins for one user accounts from two different locations/ hostnames within pre-defined time interval.

(g) Alert for any access attempts, successful login and failure to any Networking devices and their configuration changes from non-whitelisted machines.

(h) Monitoring of windows event logs of all the employer machines for setting up alerts in respect of violations to the bonafide usage i.e. Acceptable Use Policy (AUP) like what the users can or cannot do on their IT assets while configuring and managing OT/ICS/SCADA devices and networks.

(i) Set up alert for any traffic originating from unallocated IP in the allocated IP range to any host machine/ network device. Any traffic from non-whitelisted IPs in Network may trigger an alert in OT SIEM/SOC.

(j) Monitor for OT assets not being connected to the network for prolonged duration and suddenly trying to communicate with the central site. Generate alerts for such activity.

(k) Ensure that the practice of incident ticket management is implemented and strictly adhered to by all SOC team members. All tickets for incidents should only be closed after the facts have been verified.

(l) Ensure that proper timebound investigation of every alert is undertaken.

(m) For every alert generated by the SOC, ensure that the corresponding raw event log and packet capture logs that triggered the alert, is also available for investigation.

(n) Suitable alerts should be configured for timely detection of network/service enumeration attempts.

(o) Automated AI/ML/DL based threat models specific to OT/ICS/SCADA network be configured. E.g.: Normal behavior in terms of value or frequency of specific OT sensors be utilized to generate normal acceptable behavior, any deviation to the same should be raised an alert to be investigated by SOC analyst.

(p) Usage of AI/ML components for triggering alerts in respect to beaconing/robotic and rarity-based anomalies in the BESCOM OT network should also be configured.

(q) All the event-Ids (***for windows***) to be monitored in the SOC in respect to all the systems/servers for ruling out any intrusion/abnormality is enclosed at **Appendix – 'II'**. Similarly, approach should be followed for Linux, Mac based or any other customized/proprietary OS also.

3. Following data from endpoints is required to be fed & analyzed in SIEM / SOC data lake.

- List of Running services
- Parent-Child Process Trees
- Integrity hash of background executables
- Installed applications
- Local and domain users
- Unusual authentications
- Nonstandard formatted usernames
- Listening ports and associated services
- Domain Name System (DNS) resolutions
- Settings and static routes
- Established and recent network connections
- Run key and other autorun persistence
- Scheduled tasks
- Artifacts of execution
- Event logs
- Antivirus detections
- Operating system logs-Sysmon, WEF, Syslog, SNMP, WMI, PowerShell
- Firewall, UTM, WAF and DNS Debug Logs
- Volatile Artifacts- Temporary artifact collected from endpoint data sources for the purpose of hunting that might not touch the disk on the host Data Collection: Memory, Network Conn, Process Conn
- Non-Volatile Artifacts: Artifacts that reside on endpoint / hot disk
- Data Collection: Prefetch, Amcache, Shimcache, MFT, Registry, bash_history, Task Scheduler

4. Following data available in the organization should be categorized for understanding adversary behavior:

- PowerShell logs

- SSL/TLS inspection
- System Calls
- Antivirus
- Application logs
- Binary file metadata
- DLL monitoring
- Kernel Drivers
- Loaded DLLs
- Malware reverse engineering
- NIDS
- Network Protocol Analysis

33.SERVICE LEVEL AGREEMENT

1. BESCOM will provide the required information/data and access to perform the said services.

2. The tenderer and all the personnel engaged in the activity has to execute the Non- disclosure agreement with the BESCOM before collecting any information/data pertaining to the activity.

3. The tenderer will be responsible for making his own arrangements for all his accommodation, travel, transportation etc. to carry out the activity.

3. Service Level Agreement (SLA) Compliance and Penalty Clause:
The Tenderer shall ensure the minimum monthly service availability for each deployed system/tool including SIEM, SOAR, NBAD, UEBA, WAF, EDR and related components, as per the agreed SLA. SLA compliance and service availability shall be measured solely on the basis of system-generated, time-stamped and tamper-proof SLA reports generated by the respective tools themselves, and such reports shall be final and binding for the purposes of SLA assessment, billing and penalty determination. Any period of non-availability, partial availability or failure to deliver agreed functionality attributable to the Tenderer shall be considered as downtime, excluding only Employer-approved scheduled maintenance. Monthly payments shall be released only after validation of SLA compliance, and no payment shall be made for the period of non-availability, with proportionate deductions and penalties imposed for SLA shortfall as per the agreed terms, which may be adjusted against the monthly invoice or recovered from the Performance Security. Repeated or persistent SLA violations shall constitute a material breach of contract and may result in escalation of penalties, withholding of payments, invocation of Performance Security and/or termination of the Contract, at the discretion of the Employer.

Schedule for Completion of Tasks:

Sl No	Activity	Time period of Completion	Penalty for delay in Completion
1	Submission of Detailed Project Plan and Way forward.	15 days from date of issue of DWA	0.5% of one time set up cost for each week delay
2	SOC Facility Setup & SIEM - Design, build, and operationalize SOC room; deploy SIEM with real-time log collection & correlation	SOC room readiness & SIEM go-live within 90 days from the issue of DWA	0.5% of one time set up cost for each week delay
3	Complete Delivery, deployment, configuration, integration and user testing of the Application/Software along with license, Registry note, User Manuals and other necessary documents of the Application/software as listed below:	180 days from date of issue of DWA	0.5% of one time set up cost for each week delay
3 a.	SOAR (Security Orchestration, Automation & Response)	SOAR workflows operational within 120 days from the date of issue of DWA	0.5% of one time set up cost for each week delay
3 b.	Threat Intelligence Platform (TIP)	TIP integrated with SIEM/SOAR within 150 days from the date of issue of DWA	0.5% of one time set up cost for each week delay
3 c.	Endpoint Detection & Response (EDR)	EDR deployment within 120 days from the date of issue of DWA	0.5% of one time set up cost for each week delay
3 d.	Mobile Application Security (RASP)	RASP integration within 150 days from the date of issue of DWA	0.5% of one time set up cost for each week delay
3 e.	Infrastructure / Cloud On boarding	Integration completed within 120 days from the date of issue of DWA	0.5% of one time set up cost for each week delay

3 f.	External Attack Surface Management (EASM)	EASM tool operational within 120 days from the date of issue of DWA	0.5% of one time set up cost for each week delay
3 g.	DDoS Protection	Solution activated within 150 days from the date of issue of DWA	0.5% of one time set up cost for each week delay
3 h.	Web Application, API & Bot Protection (WAF)	WAF go-live within 150 days from the date of issue of DWA	0.5% of one time set up cost for each week delay
3 i.	Unified Endpoint Management (UEM)	Enrolment within 150 days from the date of issue of DWA	0.5% of one time set up cost for each week delay
3 j.	Identity & Access Integration (SSO & MFA)	SSO & MFA rollout within 150 days from the date of issue of DWA	0.5% of one time set up cost for each week delay
4	Deployment of SOC Resources at BESCOM premises	Within 1 week after the UAT sign off from BESCOM	0.5% of one time set up cost for each week delay
5	Handing over, Training and go-live of the final version of the application/software.	180 days from the date of issue of DWA from the date of issue of DWA	0.5% of one time set up cost for each week delay
6	Software Service/Maintenance Support: The tenderer should agree for Software Service/Maintenance support from the date of deployment of final version, testing and go live. The Software service/maintenance support should carry fixing bugs, applying patches, removing code injection; customizations	5 years after completing the initial setup.	As per the SLA clause table - 1

Service Level Agreement (SLA) TABLE -1:

Sl. No.	Scope / Component	Description	KPIs / SLA Metrics	Penalty Clause	Reporting / Governance
1	SIEM	deploy SIEM with real-time log collection & correlation	• 100% critical log sources on boarded• SIEM uptime ≥ 99.0% except updating of the tool/software.	If uptime < 99.0%: 1% of monthly charges against the tool cost. If uptime < 98.0%: 2% If uptime < 97.0%: 5%	Weekly setup-progress report; monthly uptime & on boarding dashboard
2	SOAR	Implement SOAR for automated incident response & workflow integration	• ≥ 80% repetitive incident automation• Mean Time to Triage (MTTT) ≤ 15 min• Mean Time to Respond (MTTResp) ≤ 30 min• Playbook execution success rate ≥ 95% except updating of the tool/software.	• Automation coverage < 70%: 1% penalty on respective monthly charges against the tool cost• < 60%: 2% • < 50%: 5% • MTTT > 30 min (average): 0.5% per 5 min over, capped at 5% • Playbook success rate < 90%: 1% penalty, < 80%: 2%, < 70%: 5%	Monthly SOAR-automation and response-time dashboard; SLA-breach log
3	Threat Intelligence Platform (TIP)	Aggregate & enrich IOCs, correlate with SIEM, enable threat hunting	• ≥ 3 threat feeds integrated• IOC ingestion latency ≤ 15 min except updating of the tool/software.	If fewer than 2 feeds integrated by 90 days: 1% monthly charges against the tool cost. If	Monthly threat intelligence & advisory report

Sl. No.	Scope / Component	Description	KPIs / SLA Metrics	Penalty Clause	Reporting / Governance
				IOC ingestion latency > 30 min average: 1% penalty per 15 min delay, capped at 5%	
4	EDR	Deploy advanced EDR agents across IT, OT, IoT	• 100% endpoint coverage• Threat detection ≤ 5 min• Isolation/quarantine ≤ 10 min except updating of the tool/software (no. of endpoints assigned by BESCOM)	• Endpoint coverage < 98% by deadline: 1% penalty on monthly charges against the tool cost • Detection latency > 10 min average: 1% per 5 min delay, capped at 5% • Isolation latency > 15 min average: same penalty scheme	Monthly endpoint coverage & incident response report
5	Vulnerability Management	Continuous scanning, prioritization & remediation tracking	• Critical vulnerability reporting ≤ 24 h• Remediation SLA: Critical ≤ 15 days, High ≤ 30 days except updating of the tool/software.	• Missed report latency > 48 h: 1% penalty of the monthly tool cost per day delay, capped at 5% •Remediation SLA	Monthly vulnerability posture & remediation compliance report

Sl. No.	Scope / Component	Description	KPIs / SLA Metrics	Penalty Clause	Reporting / Governance
				breach: 0.5% of monthly charges per missed ticket, capped at 10% quarterly	
6	Mobile Application Security (RASP)	Integrate runtime protection into BESCOM mobile apps	• 100% coverage for critical apps• Exploit-blocking rate ≥ 95%• False positive blocking ≤ 5% except updating of the tool/software.	• Coverage < 95% by deadline: 1% penalty on monthly charges against the tool cost • Exploit-blocking rate < 90%: 1% penalty, < 80%: 2%, < 70%: 5%• False positive rate > 10%: 1% penalty	Monthly runtime attack & block event report
7	Infrastructure / Cloud Onboarding	Integrate on-prem, private, public-cloud workloads	• 100% critical workloads onboarded• Compliance reporting enabled except updating of the tool/software.	• Less than 95% workloads onboarded by deadline: 1% penalty on monthly charges against the tool cost • Compliance reporting not enabled on any workload by deadline: 2% penalty on monthly	Quarterly compliance & asset inventory report

Sl. No.	Scope / Component	Description	KPIs / SLA Metrics	Penalty Clause	Reporting / Governance
				charges against the tool cost	
8	External Attack Surface Management (EASM)	Continuous discovery of external-facing assets, shadow IT	• Daily discovery refresh for critical assets• Exposure advisory delivered ≤ 24 h except updating of the tool/software.	• No daily discovery refresh for more than 2 consecutive days: 1% penalty on monthly charges against the tool cost per day overdue, capped at 5% • Exposure advisory latency > 48 h: 1% per 12 h delay, capped at 5%	Monthly exposure & risk-reduction report
9	DDoS Protection	On-prem or cloud-based mitigation for volumetric & L7 attacks	• Mitigation activation latency ≤ 5 min• 99.99% availability during active attack periods except updating of the tool/software.	• Mitigation latency > 10 min average: 1% on monthly charges against the tool cost per 5 min delay, capped at 5% • Availability during attack < 99.9%: 1% penalty, < 99.0%: 2%, < 97.0%: 5%	Post-incident DDoS mitigation report & uptime stats

Sl. No.	Scope / Component	Description	KPIs / SLA Metrics	Penalty Clause	Reporting / Governance
10	WAF + API + Bot Protection	Deploy web-application firewall with API and bot mitigation	• ≥ 95% OWASP Top-10 attack vectors blocked• Virtual patch deployment ≤ 24 h post-identification except updating of the tool/software.	• Attack-vector blocking rate < 90%: 1% penalty on monthly charges against the tool cost, < 80%: 2%, < 70%: 5% • Virtual patch latency > 48 h: 1% per 12 h delay, capped at 5%	Monthly WAF effectiveness & threat trend report
11	UEM	Enroll & manage all enterprise devices	• 100% device enrollment• ≥ 95% patch compliance across managed devices except updating of the tool/software.	• Enrollment < 98% by deadline: 1% on monthly charges against the tool cost penalty • Patch compliance < 90% average: 1% penalty per 5% shortfall, capped at 5%	Monthly compliance & patch-status report
12	Identity & Access Integration	Implement SSO, enforce MFA, RBAC for SOC tools	• 100% SSO integration• 100% privileged accounts using MFA• Quarterly access reviews completed on schedule	• SSO integration incomplete by deadline: 1% penalty on monthly charges against the tool cost per	Quarterly access review & compliance report

Sl. No.	Scope / Component	Description	KPIs / SLA Metrics	Penalty Clause	Reporting / Governance
				tool not integrated • Privileged accounts without MFA: 1% per 5% shortfall, capped at 5%• Access reviews late: 0.5% per week overdue, capped at 5%	

Service Level Agreement (SLA) TABLE -2:

SERVICE	SERVICE LEVEL AGREEMENT (SLA)	PENALTY
Resources Availability	All the resources shall be made available as mentioned in Detailed scope of work of Tender document.	1% of monthly charges for unavailability for a week of any one resource
Incident Response	**Providing initial response for:** Severity L1: 30 minutes Severity L2: 90 minutes Severity L3: 120 minutes **Providing mitigation plan for incidents:** Severity L1: 30 minutes Severity L2: 90 minutes Severity L3: 120 minutes	Maximum 2 SLA breaches are accepted in a month. For every single breach thereafter, penalty will be charged 0.5% of cost of monthly charges up to maximum 10% of quarterly charges.
Root Cause analysis	Providing report with root cause analysis: Severity L1: within 48 hours.	0.5% of cost of monthly charges up to maximum 10% of quarterly charges.

Reports Management	Report Type • Daily Report: Next working day • Weekly Report: Every Monday • Monthly Report: 1st of every month • Report to be submitted on next working day in case designated day is a holiday	0.5% of cost of monthly charges up to maximum 10% of quarterly charges.
Others	Customization of the Play Book as per BESCOM requirement within the stipulated time	0.5% of cost of monthly charges up to maximum 10% of quarterly charges.

Note:

- At any point in time, if the solution is not able to handle the committed EPS count, the solution will be considered as DOWN and corresponding SLAs shall be applicable.
- The tenderer is expected to improve the operations on an on-going basis. The tenderer is expected to provide a quarterly report of the new improvements suggested, action plans, and the status of these improvements to the BESCOM. The successful tenderer should conduct a quarterly review meeting with participating BESCOM officers resulting in a report covering details about current SOC SLAs, status of operations, key threats and new threats identified, issues and challenges etc.
- The time would start from the event being reported either by the service provider or BESCOM representative.
- In the event of any of the hardware/ software which is a part of the solution requiring a replacement, the replaced hardware / software needs to be of the same configuration / version or higher.

Category / severity classification:

SEVERITY	DESCRIPTION
L1 (Critical)	Incidents made up of any successful attempts to actively breach company's layered security controls and might result in major effect to jeopardize operations. For example: • DOS / DDOS on one or many of BESCOM applications hosted. • Ransomware found on one or more machines • Brute force attacks on the systems. • Unauthorized access acquired to critical systems like database. • Malware found on one or more than one system or an

	inability to contain the code. • The defacement, alteration or deletion of web-server files. • Failure/malfunction of supplied critical components/ Collector, Processor etc. EPS hitting the bottle neck and event logs getting dropped / truncated. There shall not be loss of logs or events from log collector in case of EPS hitting the bottle neck or event logs getting dropped or truncated. • Failure to collect logs from log sources • No work-around or manual process available. • Financial impact to BESCOM.
L2 (High)	Incidents that have moderate impact on operations and compromise identified but unsuccessful attempts of breach, for example: • Any incident which is not classified as "High Priority" for which an acceptable workaround has been provided by the Tenderer. • Moderate functional restrictions in the application irrespective of the cause. Has a convenient and readily available workaround. • Incidents that have moderate effect on operations and compromise identified but unsuccessful attempts to actively breach, for example: • Sophisticated malware that has been successfully contained or removed • Repeated active probes or port mappings from an external network. • Unauthorized attempt to tamper data • Malicious CNC connections that are blocked • Equipment/system/Applications issues and has no impact on the normal operations/day-to-day working.
L3 (Medium)	Events that cannot be definitely identified as attacks and have no effect / very limited impact on operations; for example: ➢ Isolated and non-repeated scans or pings from an external uncontrolled network ➢ Malware detected and removed prior to being placed on a network ➢ Logon failures and password guessing attempts on non-critical systems. ➢ Policy violation ➢ Non-Compliance Observations • All other residuary proposed solution Infrastructure not defined in "Medium Priority" and "High Priority".

Scope of Coverage

The C-SOC will cover BESCOM's **key IT, OT, and IoT applications and infrastructure**, including but not limited to the systems listed below:

Sl. No.	Application Type	Application / System
1	IT	Billing System: IPDS/WSS/Infoview Portal, GIS (Web/Mobile), FAM, and future applications.
2	IT	BESCOM Website.
3	IT	ERP System, Office 365 Email Services.
4	IT	Logsafe Mobile App, BMS – Building Management System.
5	IT	DTLMS Web/Mobile Application.
6	IT	Financial System (Web Application).
7	IT	Cash Management Application.
8	IT	EV Portal (Web/Mobile Application).
9	IoT	Prepaid Meter Infrastructure.
10	IT	GST Web Application.
11	IT	SRTPV Application.
12	IT	TRM Billing System.
13	IT/IoT	Spot Billing Device (Mobile/Web).
14	IT/IoT	ATP Mobile Application.
15	IT	Ganga Kalyana Portal.
16	IT	BESCOM Mithra Mobile Application.
17	IT/IoT	AMI Smart Meter Solution.
18	IT/OT	DAS OT System.

Note:

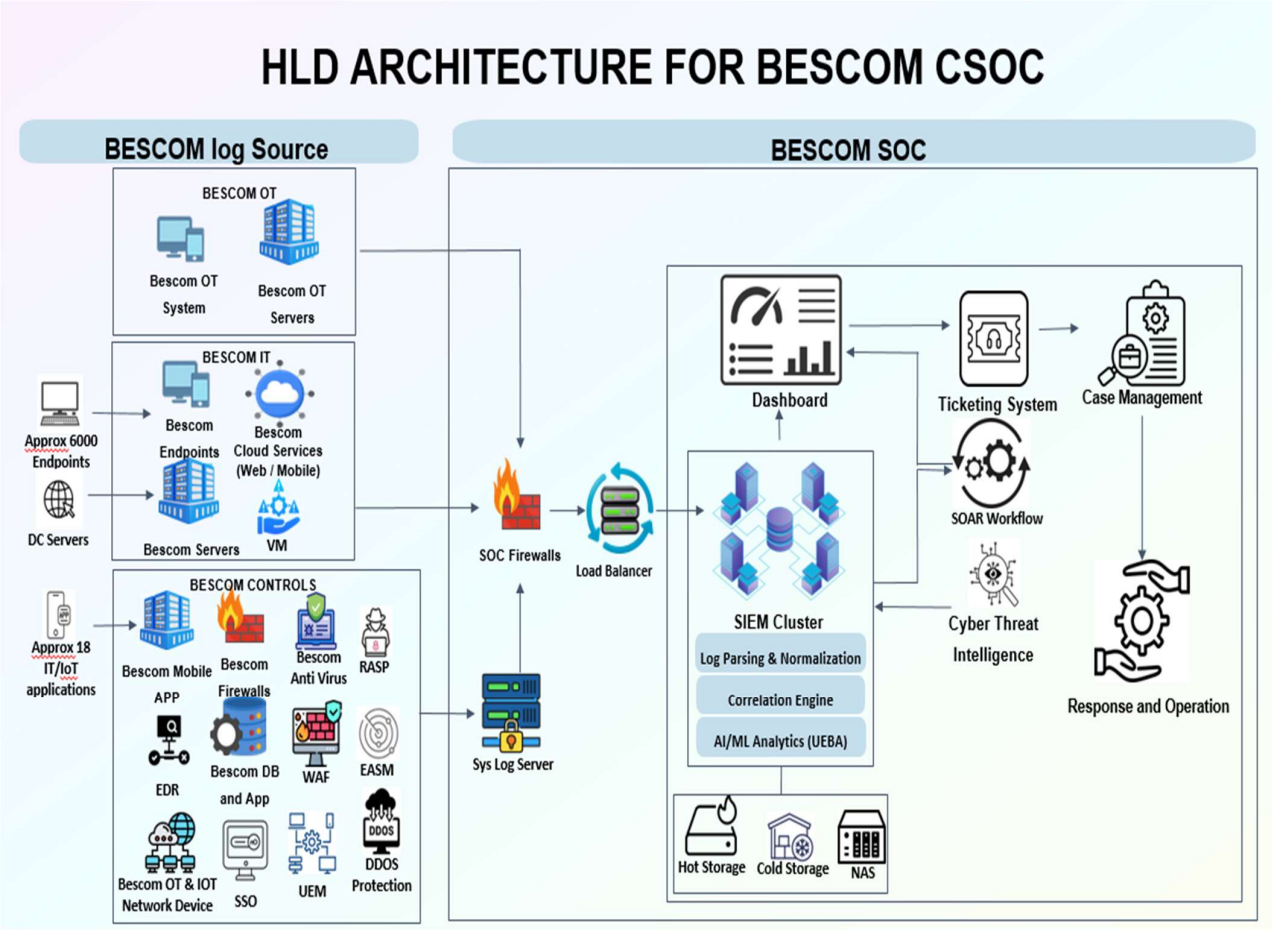
BESCOM maintains a **dedicated Data Centre and Data Recovery Centre** for IPDS Billing systems.

The IPDS Billing System, SRTPV Application, and Ganga Kalyana Application are common enterprise applications deployed and utilized across all Electricity Supply Companies (ESCOMs) in Karnataka, including BESCOM, CESC, GESCOM, HESCOM, and MESCOM.

IT infrastructure scoped in the project:

Sl No	Application Name	Log Devices	No
1	IPDS/RAPDRP	Application server (Scope may increase)	211
		Network & Security Devices	24
		Infoview Portal (8 Modules)	1
		EDR	1302
		EDR servers	4
		SD WAN devices at branch office	760
		Firewall at DC	4
		Router at DC	4
		SD-WAN at DC	2
		Switch at DC	6
		Web Gateway, URL & Content Filtering	1
		Web Application Firewall	2
		Network Load Balancer	2
		Virtual private network (VPN)	2
		Unified Threat Management (UTM)	2
2	TRM	Servers	5
		Web Application	1
		Storage, Network & Security Devices	4
3	PREPAID METER	Servers	3
		Web & Mobile (2)- Sahaj Liberty, Uemployer	2
		Network Devices	2
		Prepaid Meter Device	-
4	SBD	Servers	4
		SBD (Web)	1
		Mobile (Android)	
		Network Devices	1
5	ERP	Servers	70
		ERP Application modules (8)	8
		Network Devices	2
7	Other web applications	BESCOM Official Website	1
8	Smart Meter Devices	For web Applications	4
		Servers	7
		Network & Security Devices	2
		Smart Meter Device	-
9	End Points	Laptop/Devices	5000

High Level Diagram of CSOC Setup at BESCOM



Technical Specification

1. Security Incident and Event Management (SIEM)

Sl. No	Technical Requirements - SIEM
1	Proposed solution must be platform supporting Visibility, detection, investigation, and response
	-Gain complete visibility into security data from a single pane
	- Reduce events into a prioritized list of the most important alerts
	- Leverage AI ML models with automated, advanced analytics and threat intelligence to speed investigation time
	- Scale rapidly with out of the box use cases and integrations
	- Drive compliance and manage regulatory risk
3	Must Support a wide variety of technologies, applications, and
	cloud services to help customers gain comprehensive visibility into enterprise-wide activity
4	The solution Should include pre-built Device Support Modules, Solution must be capable of simple ingesting data from number and variety of log sources
5	Solution Must intelligently correlates and analyses a variety of data types
	from a wide range of sources, including the following:
	— Endpoint data: from the Windows event log, Sysmon, nmon , EDR solutions and more
	— Network activity data: from firewalls, gateways, routers, switches or sensors,
	— Vulnerability data: From antivirus tools, vulnerability scanners, intrusion detection systems, intrusion prevention systems, data loss prevention systems and more
	— Cloud activity: From SaaS and IaaS environments, such as Office365, SalesForce.com, Amazon Web Services (AWS), Microsoft Azure and Google Cloud
	— User and identity data, Access permissions and groups : Ingested from Active Directory, LDAP, or other identity and access management solutions
	— Application data: From enterprise resource planning (ERP) & COTS or Any other custom / in house application
	solutions, application databases, SaaS applications, Mail solution and more
	— Threat intelligence: From third-party & Open-Source threat intelligence feeds
	— Container activity data: from container management
6	Next gen Platform must include Security Big Data Lake/Central repository for security data, Security Analytics, Log Forensics, Ingestion from variety of sources including Applications, OT, IT, Network and Security with support for open choice of big data solution for future use
7	SIEM solution must apply intelligent analytics to a vast amount of security data to
	provide security analysts with actionable insight into the most critical threats, enabling them to make better, faster triage and response decisions using Agentic AI and GEN AI
8	The proposed solution should be sized for sustained data of 25,000 EPS or equivalent (1000) Gb/day at all layers but should be able to handle peak of 30,000 EPS or equivalent (1500) GB/day at all layers without dropping events or queuing events. There should be no limitation on the number of servers, users or log sources integrated with the solution and it should not have an impact on the license in case servers, users, or data source count changes, till the time data ingestion size remains as per ask
9	Proposed solution must be enterprise horizontally scalable solution with Mirco services Architecture , adavnced Analytics and predictive capabilities.

10	Data Ingestion should be fast and OEM solution must be capable of ingesting data from all IP sources also including Applications both home grown and commercial off the Shelf applications. In case of parsing requirement for any customised device or applications, it must be owned by OEM to provide same in 7 days free of cost, so that organization should not get non- compliant or should have any threats unidentified.
11	In case of any version change or version upgrade of devices, OEM must ensure data ingestion should not stop and there should not be any data loss and should be done with no/minimal downtime
12	The Proposed solution should have capability to collect logs real time from most of the standard platforms like Microsoft Windows, Linux (All flavours), MAC OS,AIX, Solaris, Firewalls, Network, other security devices or solution, identified database servers, endpoint security management servers, web application firewalls, network firewalls ,Active Directory servers, Web servers, private cloud etc. Solution must support historical data imports in any data formats with no extra cost or EPS and should be able to build correlation using the same
13	The Proposed solution should have inbuilt security mechanism for protecting itself from security attacks
14	The proposed solution should have physical or logical separation of the collection module, logging module and analysis / correlation module with the ability for adding more devices, locations, applications, etc (High availability)
15	The proposed solution must support caching mode of transfer for data collection, so as to ensure data is being logged in the event loss of network connectivity, and resume sending of data upon network connection.
16	The proposed solution must be able to collect data from new devices added into the environment, without disruption to the ongoing data collection.
17	The proposed solution must provide for secure user access via HTTPS, ssh.
18	The proposed solution must have a user-friendly interface to convert statistical results to dashboards with a single click.
19	The Proposed solution must offer all the below built-in threat detection techniques out of the box:
	1. Detect Web Application Threats.
	2.Detect APT Threats.
	3.Integrate with leading HoneyPot solutions.
	4.Integrate with leading NBAD, NDR tools.
	5.Give visibility of endpoints also by integrating with EDR, DLP, HIPS, Antivirus etc for endpoint analytics.
	6.Integrate with SOAR tools for automation.
	7.Integrate with leading Threat intelligence Platform (TIP).
20	The proposed solution must provide a query interface that allows users to search for data stored within the solution. it should provide view and api mechanism to run any custom query
21	The solution shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension with inbuilt data optimizer to optimize data while data collection itself
22	The solution should be able to part and filter logs based on type of logs, date etc.
23	The proposed solution should be able to receive, ingest and index structured or unstructured data and no events should be dropped
24	The solution must have an incident review framework for incident management. Incident review framework to facilitate incident tracking, investigation, pivoting and closure, with self feedback mechanism for marking true/false positive/finetuning
26	The proposed solution must be able to read data input from the following static log file formats:

	a. Archived Log Files (Single line, Multi-line, and Complex XML and JSON Structure)
	b. Windows Events Logs
	c. Standard Log Files from applications such as Web (HTTP/HTTPS) servers, FTP servers, Email (SMTP/Exchange) servers, DNS servers, DHCP servers, Active Directory servers, etc.
27	The solution must be able to provide the capability to fully customise alerts, reports, and dashboards to the business requirements from Application UI
28	The proposed solution must come with out-of-the-box integration and dashboards, reports, rules etc to provides rapid insights and operational visibility into large-scale Unix and Linux environments machine data: syslog, metrics from log data.
29	Solution must be capable of providing real time and on demand access to data sources such as evolving format, Custom API's, interfaced incl. text, XML, JSON, Data Base connections, Network Ports, Connections or from log data., and files
30	The solution must be able to provide the capability to annotate events, modify status, build a chronological timeline for the incident before and after a triggered event.
31	The proposed solution must be able to run any search on a schedule and set alerting conditions based on thresholds and deltas in the number and distribution of results across a time range or days like a histogram visualization.
32	The proposed solution must support viewing of the same log data in different formats or should support multiple schema views during search time or report building time without redundant storage or reindexing so that complex report or user defined reports can be built.
33	The solution must be able to support the following indicators:
	- Network, IP
34	- HTTP Referrer, User Agent, Cookie, Header, Data, URL
	- Domain
	- Endpoint
	- File Hash, Name, Extension, Path and Size
	- Registry Hive, Path, Key Name, Value Name, Value Type, Value Text, Value Data
	- Process Name, Arguments, Handle Name, Handle Type
	- Service Name, Description
	- Certificate
	- Certificate Alias, Serial, Issuer, Subject, Start Time, End Time, Version, Handshake Type, Public key Algorithm, Signature Algorithm
	- Email
	- Email Address, Subject Body
35	Solution should support machine learning auto triaging & manual triaging of alerts from number of security products including SIEM, DLP, IPS, WAF, Anti-APT, AV, EDR, Firewall (all with Well Known OEM's as well as Open source platforms).
	Solution should support AI and machine learning driven triaging algorithms that considers contextual parameters, historical behaviour, and external threat intelligence to enrich and arrive at a triage score in real time. Triage score should form the basis for prioritizing the alert and further action on the same
	· Environmental parameters should include and not limited to asset criticality, user criticality, and vulnerability status for every alert.
	· Historical parameters should include and not limited to attack volume, attacker volume, destination volume for every alert, severity of alert and so on.

	· Central Threat Intelligence feed should also be applied to identify threats through known bad actors
36	Solution should support a rule engine for users to define custom triage rule. Rule engine should support asset data fields, event data fields, user data fields, triage score, and triage parameters . it should be configurable from UI without any restart of services
37	Solution should have features to analyse impact of the attack on the targeted asset including configurations, Indicators of Compromise (IOCs), external network connections.
38	The proposed solution must support real-time remote indexing of data sources to minimize the opportunity for alteration of audit trails on compromised hosts.
39	Solution should support models to build up the entire attack chain from attack inception, progress of the attack and spread to attack in the network.
40	The proposed solution should be able to receive, ingest and index structured or unstructured data without schema or normalization and no events should be dropped if
41	Solution should support features to identify attacker attributes including threat intelligence score of attackers, who-is lookup information, geomapping in a single console.
42	Beside event matching signature use cases, the proposed solution must have the following analytical capabilities to address anomalies and behavioural based use cases.
	-Basic Statistical analysis that can be applied to any fields like calculating the length of command line arguments, HTTP user agent string, sub domains, URLs, standard deviation of count of events over time
	-Using distance formula to detect geographically improbable access
	-To measure the randomness of domain names that can be potentially from malware domain generated algorithms.
43	Solution should support integration with any number of open source or commercial IOC sources available today or in future. Solution should support features to analyse and identify the impact of this attack on other assets.
44	Solution should provide features to do free flow visual analysis of alerts and logs from integrated data sources based on custom criteria. This visual analytics feature should have appropriate graphical representation options to visualize large scale data.
45	The proposed solution must come with pre-packaged alerting capability, flexible service-based hosts grouping, and easy management of many data sources, and provide analytics ability for security alert in Window Unix and Linux environment. to quickly identify performance and capacity bottlenecks and outliers in Unix and Linux environment.
46	The solution should have high availability feature built in for automated switch over to secondary collector/integrator in the event of primary collector failing. No performance degradation is permissible even in case of failure
47	Solution should capability to filter undesired, non-security logs at collection, processing, and visualization layer
48	The proposed solution must be able to read data input from the following static log file formats:
	a. Archived Log Files (Single line, Multi-line, and Complex XML and JSON Structure)
	b. The solution must be able to accept the following live data streams from cloud server less functions like raw or JSON formatted data over HTTP/HTTPS.

49	The proposed solution should be able to consume logs from any log source without writing parser beforehand or while integration. Parsers should be built once log is ingested (Note: there should not be any drop of events/data. Such events/data can be parsed once parser is ready)
50	Solution should provide capability to search raw and indexed logs as full text, natural language, time range values, IPs, IP subnet mathematical & statistical functions, logical operators, occurrences count, regex, similar events, first & last seen, predictive & prescriptive search suggestions etc.
51	Solution should be capable of retrieving the archived logs for reporting, analysis, correlation, investigation, and forensics.
52	The report should be parameterized, and the user should be able to scale the parameter as needed and Out-of-box aging analysis of incident should be available. Solution should support dynamic reports scheduling and prioritization.
53	The solution should provide detection/correlation of logs with malicious IP's / hosts / Domains / sites /IOC's (leveraging external/Third Party/Open-Source TI feeds)
54	The solution should have a centralized correlation engine and a management center/console which allows creation of an unlimited number of correlation rules
55	The solution should be able to perform different correlations (but not limited to): Rule based, Historical based, Heuristics based, Behavioural based, etc., across different devices and applications
56	The solution should have the ability to correlate all the field present in a log/flow data.
57	The solution should provide a web-based, user-friendly console or a wizard- based console to create rule.
58	The proposed solution must come with out-of-the-box integration and dashboards, reports, rules etc. to provides rapid insights and operational visibility into large-scale CentOS, Windows, Unix, and Linux environments machine data: syslog, metrics from log. and configuration files.
59	The proposed solution should have the ability to perform free text search on events, incidents, rules, and other parameter
60	The platform should provide the capability to use Machine Learning models on the data, peer groups, watchlists and multple risk profiles
61	The data storage and indexing component should provide the ability to scale "horizontally", meaning the capability to start with a set of nodes within a single data store/cluster and keep adding additional nodes to handle larger volumes of data without having the need to replace or upgrade the existing nodes in the cluster.
62	The solution should also be capable of collecting and indexing machine data from all the log sources including OS platforms, Middleware, Databases, network & security devices, applications etc., and allow for collecting, indexing, searching, monitoring, and analysing logs in real-time
63	The solution should have an inbuilt parsing mechanism available in UI to be able to parse the logs obtained from multiple log sources (in the cloud and on-premises) including OS platforms, network & security devices, applications, IAM systems etc. and convert them into a standard log format on which the analysis can be done. Custom parsing shall also be available for custom applications, if out of the box parsing is not available.
64	The solution should have the capability to add as many fields/columns in the index. The solution should support any number of fields in a particular row of data and should be able to store any amount of data in a particular field
65	The solution must provide drill down functionality that is user defined, allowing users to drill down into another report, dashboard, raw events or passing url parameters to any third-party website. The Report should be scalable IP-wise, device-wise, user-wise, data-wise, location-wise based on requirement between any two dates.

66	The solution should have pre-defined rules for conducting intelligent analytics on real-time and historical log data obtained from multiple log sources (in the cloud and on-premises) including OS platforms, network & security devices, applications, IAM Systems etc. as well as threat feeds obtained from different sources
67	The proposed solution should have AI ML capabilities.
68	The solution should offer the flexibility to develop customized correlation rules for conducting intelligent analytics on real-time and historical log data obtained from multiple log sources on multiple parameters (like Hosts, Geographies, recurring activities) including OS platforms, network & security devices, applications etc. as well as threat feeds obtained from different sources
69	The solution should have capability of conducting detailed analytics, business intelligence analytics, machine learning, pattern analysis, trends & spikes, anomaly detection, access outlier analytics,etc
70	The proposed solution should also guide administrator on data sources required to implement detection technique from the same console (ATTACK MITRE/CIS/NIST/ Kill Chain etc)
71	The solution should have capability of conducting search across real-time and historical data as and when required with no limitation on date range
72	The proposed solution must provide the following capabilities as a Security Analytics Platform:
	a. One single syntax that can be used universally for search queries, alerts, reports, or dashboards, SIEM, SBDL.
	b. Incident management technique to facilitate incident tracking, investigation, pivoting and closure
	c. Risk management technique to apply individual risk scores to any asset or user based on relative importance or value to the business.
	d. Threat intelligence technique that automatically collect, aggregate, deduplicate indicators of compromise from threat feeds
73	The solution should have monitoring and alerting capabilities for individual and correlated real-time events
74	The solution must detect and alert on following:
	- Firewall port scans
	- Brute force attack
	- Network intrusions or suspect traffic
	- Backdoors and Trojans connections
	- Connect to/from bad/blocked URLs - Analyse web proxy data for connections to malicious URLs
	- Emerging Threats
	- Detect and update on emerging threats
	- Notify security incidents via Voice/Portal/Email
	- Daily/Monthly report on security monitoring service
	- Alert in case unavailability of event logs from registered device
	- TOR, DNS tunnelling kind of malicious communications
	- DNS query for malicious domains.
	- Detect suspicious object that are embedded within files through malicious
	PowerShell scripts for opening a command shell
75	Solution must provide capability of Log Filtering all logs are not needed for the compliance requirements faced by organization, or for forensic purposes. Logs can be filtered by the source system, times, or by other rules defined by the SIEM administrator.

76	The solution should provide a pluggable framework to make use of APIs. The framework should support ingestion of data from other applications, export of data from the solution using APIs as well as orchestration of triggers. This solution should provide the ability to use this capability to integrate with other applications for automating tasks and workflows.
77	The proposed solution should provide end-to end capability to setup an Analytics Platform for storage, indexing, searching, analysis, correlation, reporting, visualization, orchestration of different types of structured / semi structured data generated within the organization.
78	The proposed solution must be able to index all data from any application, server or network device including logs, configurations, messages, traps and alerts, metrics, and performance data for industry relevant formats so that the analyst can have end to end visibility of the ecosystem.
79	The proposed solution should provide dashboards for insight into resource consumption of desired systems, service availability status of critical services, integration with NMS tools for network status visibility, security alerts, risky users & entities, anomalies, and outliers across all the data etc. into a single dashboard available from log data.
80	The proposed solution must possess built-in/integrated feature for anomaly detection:
	a. Uses historical data as a baseline to forecast future patterns, thresholds, and tolerances
81	Dynamic, intuitive, parameterized, and customizable dashboards should empower personnel resources in the SOC to take prudent decisions. Multidimensional, analytical, trend &pattern-based dashboards should be recommended by individual technology based on their own self-learning capability.
82	Solution should have end to end security mechanism to ensure security of logs, data, information, alerts, users, configurations etc. at rest / storage / database, during processing and in transit.
83	Solution should have capability to receive, ingest, index structured, semi structured, unstructured data and transform, aggregate, and analyse structured data for security monitoring.
84	Solution should be capable to monitor and notify whenever any asset integrated with it stops sending logs/ events / flows/ data / traffic /TI etc.,
85	Solution should be able to provide raw and normalized logs/data storage as per the retention requirements for SIEM technology as outlined in the scope of work in this RFP
86	Solution should be capable to correlate events, network activity data, alerts, and vulnerability data to provide complete view of security threats and generate real-time security alerts
87	The proposed solution's detection use cases should be comprised of guidance that provides an assessment of the Security Threat and how it helps detect and investigate it using the proposed solution. In addition it should provide a summary of how the attack or detection technique maps to any of the following:
	--ATT&CK MITRE, an adversary behaviour model that describes the actions an adversary might take.
	--Kill-Chain, a model that identifies the phases an adversary must complete to achieve their objective.
	--CIS Critical Security Controls
	--Data types that are referenced within the rules/search and that need to be populate
	--There should be template to upload advisories in an automated manner.
	--There should be templates to design and trigger work flows automatically.
	--Any other customizable templates as per department requirements.

88	Solution should support multi-tenancy feature with segregation of data and display for different entities.
89	Raw, normalized correlated logs shall be stored to the attached storage/SAN/NAS for the future reference and forensic activities in the event of incident.
90	Solution must be able to store log data both locally and with SAN/NAS integration.
91	The solution should support UI based data masking and unmasking , it should have RBAC control for Data view based on role
92	Solution must be IPV6 ready.
93	Solution shall provide real time threat intelligence from at least one commercial and one open-source feed
94	Solution must retrofit with any legacy application/ devices/ equipment event sources, which may or may not be able to push logs. It shall be capable of collecting events from all Applications/ devices/ equipment event sources.
95	Solution must be horizontally and vertically scalable to support increase in EPS/data
96	The proposed solution should provide more than 90 percent compression on queryable data and should allow historical log exports of raw logs from big data solutions
97	The solution should support an integrated MITRE Framework and provide an interface to visualize all the various correlation rules deployed in the SIEM and their mapping with the MITRE framework to evaluate whether all TTPs on the MITRE framework have been adequately covered with rules.
98	The solution should be able to identify the common sources or targets across all the alerts raised historically and also identify how many alerts have been raised by these common sources or targets.
99	The solution should also correlate the alerts and give a view of the entire threat campaign to the user for quicker analysis and reducing alert fatigue.
100	Solution should support creation of customized reports in formats like csv, doc and pdf with custom logo of the organization.
101	Solution should be able to integrate with security devices like Firewall, IPS, endpoint Security solution, APT solution, WAF etc. from day one. Solution should support integration with third party OEM products including but not limited to the following technologies:
	a) Forensic tools,
	b) IT (e.g. AD, SAML),
	c) SIEM Solution,
	d) Communication tools (e.g. Email),
	e) Endpoint Security Solution,
	f) Network Security Solution,
	g) Threat Intelligence,
	h) Dynamic malware analysis.
102	Solution should support Dashboard and any Dashboard which can be provide high level view of Platforms KPI's.Dashboard should be exportable, RBAC controlled and should have facility to email dashboards periodically
103	Proposed SIEM solution should have capabilities to be integrate with SOAR, EMS/NMS, ITSM etc.
104	The solution should be able to access structured data in your logs without extraction
105	The solution should be able to access structured data in your logs without extraction

2. SOAR (Security Orchestration, Automated and Response) &Threat Intelligence Platform (TIP)

Sl.No	SOAR & TIP Requirements
1	Solution should be able to deploy on-prem virtual machine or cloud-based with the same license.
2	Solution should run the scripts/integration modules/action processors inside dockers & containers to protect the system from executing malicious scripts or harmful commands.
3	The solution should support User authentication via LDAP and SAML, SSO, AD, etc.,
4	Solution must be web based without the need for installing an additional client software for administration and routine day to day usage requirements.
5	The solution should support Role-Based Access Control (RBAC) mechanism for incident and other related system data which defines the segregation of duties.
6	Solution should support deployment for access remote networks which are behind the firewall or isolated from Internet
7	Solution should support backup/restore and provision for creating a HOT backup/standby server.
8	Solution should provide new content pack which includes new feature upgrades on a periodic basis free of charge.
9	Solution should have provision for storing security incidents/alerts and related artefacts for minimum 36 Months. Data retention & data archival settings should be or configurable.
10	The solution must have a web-based GUI for analysis, reporting and other management activities.
11	For audit reasons, the solution must be capable of logging all failed attempts to login into the user console.
12	Solution should support periodic reporting and compilation of evidence for audit requirements
13	Solution should provide reporting/dashboard functionality to fetch security incident report based on incident category, incident status threat score, threat intelligence inputs, specific asset. specific agency, time duration, criticality/severity, creation date, closure date, etc.
14	Solution should provide automated incident SLA breach report based on severity, type, creation time, closure time, response time, etc.
15	Solution record audit trail of all manual and automated steps, actions during execution of a playbook.
16	Solution should provide management summary dashboard with information like statistics about incidents, solution effectiveness in terms of cyber incidents handling times, etc.
17	Solution should support creation of customized reports in formats like csv and pdf with custom logo of the organisation
18	Solution should support creation of customized widgets based on the requirements. These widgets should then be allowed to add to dashboard and exportable in report in formats like csv and pdf with custom logo of the organisation
19	Solution should have integration support for various network and security solutions not limited to Firewall, SIEM, IPS/IDS, EDR, ITSM and WAF.
20	Solution should be capable of implementing a new integration without any coding requirment and should support no code based implementation.

21	Solution should auto-assign a unique ID to every incident/case that has been ingested into the system
22	Solution must provide UI based wizard to manually create incidents.
23	Solution should support creating an incident/case based on an email input, XML, Manual entry, URL, An API Call, Ticketing system, Custom portal (WebForm), Syslog, free text, JSON etc.
24	Solution should allow an analyst to upload file attachments as artifacts, evidence etc. / should not get deleted or modified once added
25	The solution must provide central management of incidents and administrative functions from a single web-based user interface.
26	Solution should track all forensic data related to an incident in one location (s system images, snapshots etc) and view the history of evidence across the entire incident
27	Solution should support updating existing out of the box integration and allow addition of new tasks without any coding requirement.
28	Solution should have capabilities to map the incident automatically as well as manually to MITRE ATT&CK navigator
29	The solution should have capabilities to map the incident, attacker, TTP and software data to the MITRE ATT&CK navigator
30	The solution should have capabilities to correlate between the Incident, IOC, TTP, malware family and Threat actor within the platform
31	Solution should use playbooks/runbooks with an editor which supports visual creation of playbooks without the need to code by native integration to third party tools and processes
32	Solution should have the ability to suggest malicious phishing emails based on machine learning.
33	Solution should allow creating new playbooks to map out the CIRT (Computer Incident Response Team) processes. Provision for building min 100 custom playbooks should be factored within the solution and should be scalable upto 150 custom playbooks.
34	Solution should support reuse of existing task, and should provide capability to use nested playbook (playbook inside another playbook) to enrich incidents or resolve incidents.
35	Solution should support out of the box playbook mapped to all the MITRE Tactics
36	Solution Should allow creation of Manual Tasks, Automated Tasks and Conditional Tasks in Playbooks
37	Solution should allow a single playbook to have Automated and Manual Tasks within the same playbook
38	Solution should allow a complete playbook to be run automatically or manually and list out any exceptions
39	Solution should record all manual and automated entries during execution of a playbook
40	Solution should allow addition of adhoc tasks within a playbook
41	Solution should support running playbooks as scheduled tasks at pre defined time intervals
42	Solution must support provision to pass parameters to upstream/downstream task within a playbook
43	The solution must have a mechanism to save and maintain multiple versions for the playbooks

44	The solution should allow for viewing all or selected playbook and provide option for restoring to an older version
45	Solution should support sending notifications to other users on playbook failures.
46	Solutiion should be able to embed custom code into playbooks using custom utils.
47	Solution should support implementing custom util using python , these utils should be allowed to be tested against the alert data at the time of creation.
48	Solution should allow including multiple custom utils in one utility and allow logging the information from multiple utils.
49	Solution should allow automatic execution of playbook on the grouped cases and should allow automatic execution of playbook on the cases which are not grouped via the group rule
50	Solution should be able to perform the enrichment using the integrated tools automatically for all the ingested alerts.
51	Solution should support the tracking of the assets involved in one incident at a central place along with all the security control mapped the particular asset
52	Solution should support the central tracking of all the assets involved within the incidents along with their current investigation status
53	Solution should be able to map user/department/location/asset information to the incident
54	The solution must be capable of securing and managing every type of asset such as servers, applications, endpoints, software and users related to the incidents being investigated.
55	Solution should facilitate correlation of malicious campaigns by connecting the dots between incidents, vulnerabilities, threat actors, malware, and assets.
56	Solution should be able to track the users involved in an incident along with providing details of the user present in the incident.
57	Solution should be able to identify coverage gaps by identifying missing mandatory controls in the environment.
58	Solution should have a feature of auto assignments of calls to analyst on the basis of complexity of case and availability of engineers in the shift
59	Solution should allow scheduling of playbooks to allow execution at specific time along with scheduling of reports to be sent across recepients.
60	Solution should allow running queries on the cases to fetch the cases depending on the analyst requirement.
61	Solution should support various structured and unstructured Threat Intelligence feed formats gathered from a combination of Commercial, Open source, User-led, and Community-driven Intel sharing sources and also provide complete advisory of threats to enable the organization to plan countermeasures for taking proactive actions.
62	Solution should support all the STIX objects out of the box and any feed ingested should be converted to STIX objects
63	Solution should support open standard formats like CyboX, OpenIOC, Yara, STIX 1.0, STIX 2.0, MISP, XML, CSV, JSON, MAEC, IODEF etc.
64	Solution should also be capable of supporting unstructured formats such as email, news, RSS Feeds, blogs, Free text etc. and should be capable of automatically normalizing it.
65	Solution should have the ability to import and export Intel feeds in popular consumable formats such as XML, JSON, CSV, etc.
66	Solution should be able to perform Normalization - Consolidating data across different sources formats.

67	Solution should be able to do De-Duplication - Removal of duplicate information.
68	Solution must provide additional information on IOCs, wherever requested, by integrating with WHOIS, Virus total, Shodan, Hybrid Analysis etc.
69	Solution should support scoring of feeds or IOC to ensure only relevant feeds are worked upon by the analyst.
70	Solution must be capable of ingesting vulnerability data from various sources to correlate during the incident investigation
71	Solution should support automated indicator deprecation, in which the indicator gets expired after the decided time-span. The platform should also have an option to auto unblock IOC on deprecation.
72	Solution should allow the analyst to mark the severity and risk, track and add comment/notes for the indicators.
73	Solution should support interactive analysis with help of notes/ comments which can be shared with other analysts.
74	Solution must support Threat Intelligence sharing format/protocols such as STIX/TAXII.
75	Solution should record timestamp for all actions taken in an incident.
76	Solution should have an incident analysis structured process to identify the source and the cause of incidents, analyse the extent of compromise for quick containment and minimize losses.
77	Solution must be able to correlate an existing incident with a historical one if there is a match
78	Solution should perfomr parsing all the SIEM message fields, including but not limited to: creation time; update time; source/dest IP; source country; category; system; rule-name; severity; dest IP
79	Solution should be able to whitelist/blacklist IOCs on the platform and track the IOCs depending on the IOCs mentioned in the whitelist/blacklist.
80	Solution must capable of publishing its own health reports for administration and maintenance
81	Solution should have an option to configure and manage the SOC shifts within the platform
82	Solution should support customizable dashboards for different roles and access levels.
83	The service scope for initial deployment should include integration with out of box products as well as to build custom integrations(5) along with customization of reports/ dashboards/ queries etc.

3. Cloud WAAP Technical Specifications alogn with Anti DDoS

S.No	Description
1	The proposed Cloud Application Security Service should support minimum 10 Applications with at least 200 Mbps HTTP/S traffic from day 1 (Committed at any given point of Time) and no restriction based on Data Transfer and policy change. Proposed solution should have provision to scale up traffic and applications, if required in future wihtout any impact on the production.
2	The WAF and Anti-DDoS services shall be integrated to ensure seamless security with high efficiency and shall be from same OEM. Further, no separate traffic redirection shall be configured by BESCOM for WAF and Anti-DDoS services.
3	Cloud WAF, API Protection, BOT Management, DDoS Mitigation services should be from the Same Technology OEM.
4	Should have at least 50+ PoP's globally and minimum 2 Point of Presence should be available within INDIA.

5	The solution should support Nokey feature so the CWAF service can integrate with HSM and onboard BESCOM applications without private key upload to the cloud, so if BESCOM decides they can maintain exclusive access to the private key, securely stored in Hardware Security Modules (HSMs).
6	No hardware & software is to be installed at Origin Web server/DC for the provisioning of the Cloud WAF security services. However, for Internal Applications that are not exposed publicly, The proposed solution should also support an out-of-path API-based cloud application security architecture to optimally protect internal applications deployed in Datacentre which cannot be DNS routable over the internet (using same WAAP service plan) . This service should integrate on-premise load balancing or reverse proxy solution (including Radware, F5, Ngnix, HA Proxy etc). via plugin/connector.
7	The proposed solution should support threat intelligence feed a which should automatically block attackers with bad reputation.
8	Solution should offer feature to control SSL/TLS Version via Cloud WAF. It should provide support for SSL/TSL Version such as SSLv3, TLS 1.0, TLS1.1, TLS 1.2 & TLS 1.3.
9	The proposed WAF Solution must also have the capability to import both Certificate and Private key of the Application. This is to ensure that same certificate is used on the server and on the WAF Solution.
10	It should allow to configure a custom security page to be displayed to visitors who are violating the web application and API Protection security modules.
11	The CWAAP solution should allow to address false positives of application-level attacks in a simple, self-service action, through the Cloud portal.
12	Solution must be able to protect applications regardless of the location of origin server. The origin server can be present in public cloud, private cloud or on-premises datacenters. The offered services must be able to protect both HTTP and HTTPS (SSL) web applications.
13	The proposed solution services must have provision to Load Balance & Failover across Origins (DC-DR) in the form of an Add-on feature. The Proposed Solution should support : 1. Round Robin and Least connection to load balance the traffic between Origin Servers. 2. Load balancing between atleast 8 origin servers. 3. Cookie and IP based Persistency.
14	The solution must have the capability to perform URL-based redirection and Modification rule: : Location: the location in the URL to look for the condition (URI, Header, Parameters, or IPs Groups) Condition: can be Starts with, Contains, End with, Equals to, Does not start, Does not contain, Does not End With, or if the location was IPs Groups, this can be Contains IP. Value: for URI this is part of a URL address, for Header this is the Header name or value, for Parameter this is a Parameter example, for IPs Groups you must select an IPs Groups from Templates and Policy section.
15	It must be able to prevent all application security threats including SQL Injection, Cross-site Scripting (XSS),Remote File Inclusion (RFI), Local file inclusion (LFI), Cross-site Request Forgery (CSRF),Server-side request forgery (SSRF), Protocol Attacks (HTTP RFC Violation Protection), Brute Force Attacks, Predictable Resource Location, Buffer Overflow, Code Injection, Command Injection, SSI Injection, LDAP Injection, Clickjacking, Path Traversal, Information Leakage, Directory Indexing, Common Vulnerabilities, Security Misconfigurations, Path Traversal, Request Tampering, Parameter Pollution,Parameter Manipulation, Broken Object-Level Authorization, API Abuse, Man-in-the-Middle (MitM) Attacks.

16	The proposed solution should have an ability to temporarily block source IP from any activity as a penalty for continuous security violations. The Solution should have user configurable policies including : 1. Sensitivity Level— Sets the sensitivity level of this feature : Low, Medium, High,or Custom) 2. Blocking Time - The amount of time an individual source is blocked (Minutes,Hours) 3. Exclude IP s List
17	The proposed solution support below rules : • Redirect Rules - redirect traffic to a maintenance page • Security Rules - prevent search engine bots from accessing a website or block access to specific sections of a website based on IP address or Headers • Delivery Rules - change the value of a header to another value, or remove the header • Response Delivery Rules - add an additional header to specific requests
18	The solution must be able to detect and block attempts to bypass geo-location rules through TOR and anonymous proxies etc.
19	The proposed solution shall provide protection templates that allow defining a set of security mechanisms once and reusing them across multiple applications within the account. This eliminates the need to manually configure protection settings for each individual application, thereby improving efficiency and consistency.
20	The proposed solution should have the provision for version control capabilities for security configurations. Each time changes are applied to a Security Policy, a new version must be automatically created so that we can restore or revert to previous versions if needed and maintain a clear history of changes.
21	The Solution should support a “Diff” feature that shall be available on the portal to visually compare differences between the current production configuration and prior versions, facilitating easier understanding of changes.
22	The proposed solution shall provide centralized security management capabilities, enabling the assignment and application of security configurations to multiple applications simultaneously. This functionality shall streamline the management of security policies across a diverse portfolio of applications, improving operational efficiency and consistency.
23	It should preferably allow to configure a custom security page to be displayed to visitors who are violating the web application and API Protection security modules.
24	The proposed solution must offer feature to control SSL/TLS Version via Cloud WAAP. It must have support for SSL/TSL Version such as SSLv3, TLS 1.0, TLS1.1, TLS 1.2 & TLS 1.3.
25	Should provide Service Level Commitment of minimum 99.999% at least with Service Credits
26	WAF supports HTTP/HTTPS ports along with the Customized Ports inspection using a non-standard ports range between 1024 and 65534
27	The Proposed solution should provide its own self generated managed certificates for the applications. It should automates the process of generating, renewing, and managing domain certificates, eliminating the need for manual intervention. The Proposed solution should generate individual SSL certificate for each domain or sub-domain, it should not use any wildcard certificate.

28	The proposed solution must have the provision to offer Client-Side protection as an add-on to safeguard end user data from client-side attacks, including data leakage, formjacking, Magecart, supply chain, e-skimming, and DOM-based XSS for legitimate and unknown destinations. Client Side Protection should provide continues discovery and monitoring of all 3rd party services including detailed activity tracking. It should features: • Threat level assessment according to multiple indicators • Ability to block malicious domain and allow legitimate domains with exception • Real time notifications for every new discovery and changes in existing services It should also show the destination domains to which the outgoing requests are sent and presents various characteristics about the domains that have been detected along with Discovered date, Last Seen, Certificate, threat Level, script, visitors, domain status etc.
29	The proposed solution should have the provision to provide Web DDoS Protection as an add-on with following features & functionalities, this capability should be made available as an optional enhancement, which can be enabled based on specific business needs. 1. Behavioral-based detection with self-learning and autotuning 2. Real-time automated Signature generation, Layer 7 signature should be visible as part of security logs on the Unified portal. 3. Granular enforcement with no false positives 4. Combines both rate-based and behavioral parameters 5. Identifies attacks even if they don't cross volume threshold 6. Distinguishes between attack and legitimate rise in traffic (e.g., holiday shopping peaks) 7. Automated, real-time signatures tailored to attack characteristics 8. Applies L7 logic, with up to 40 separate HTTP/S parameters 9. Dynamically adapts to changing traffic patterns, without any manual intervention. 10. Automatically deployed and mitigates attacks with no human intervention required
30	The proposed solution should support BOT Management capabilities for applications.
31	The Bot mitigation must accurately distinguish incoming traffic between human and bot traffic and identify "good" and "bad" bots.
32	The Proposed OEM have the provision to Detect and identify bots using a multi-layered approach options for bot mitigation which includes block, feed fake data, CAPTCHA, throttle, drop, session terminate, redirect loop, log only, Crypto Challenge and custom actions. This capability should be made available as an optional enhancement as an add-on, which can be enabled based on specific business needs.
33	The Solution should support crypto mitigation algorithms as an optional add-on if needed that provides an option to enable genuine website visitors to enjoy a frictionless, CAPTCHA-free user experience.
34	If needed, with an optional add-on the Solution should support captcha less crypto challenges for the BoTs by sending CPU-intensive browser-based challenges with gradually increasing difficulty, forcing the attacker's CPU to work harder every time it is challenged, eventually choking the device. Provides. This feature enables genuine website visitors to enjoy a frictionless, CAPTCHA-free user experience.
35	If needed, with an optional add-on the Solution should support the Solution should include support for device attestation with Google (Android) and Apple (iOS) devices for tighter & faster protection of mobile application. Solution should be capable to check the device authenticity, ensuring that only real devices get access to mobile application and resources, blocking app emulators, modified applications, and applications with modified OS.
36	The proposed solution is required to facilitate seamless integration of the SDK with Native Platform, to enable the SDK to be integrated with a much broader range of customer mobile applications thus extending the bot protection capability across all of these applications.

37	The Proposed Solution should Support API Security features such as : • Schema enforcement for documented REST API • Schema enforcement for documented GraphQL API • Protection attack embedded • API Protection against Automated Threats • Data leakage Prevention • API Quota Management
38	Proposed solution should have capability to Detect and identify bots using a multi-layered approach option for bot mitigation which includes below mitigation options a) Allow, b) Block, c) Drop, d) Session terminate, e) log only, f) Custom Response.
39	If required, the proposed solution should have the provision to support comprehensive Business Logic Attack (BLA) protection with real-time mitigation Business Logic attack mitigation capabilities. It should continuously analyze API transactions across all users and endpoints to detect and prevent business logic vulnerabilities.The solution should leverage advanced AI to learn normal behavior patterns and automatically create precise security policies. These policies must effectively detect detect and block malicious activities without impacting legitimate user traffic. This capability should be made available as an optional enhancement, which can be enabled based on specific business needs.
40	The solution must have multiple methods for Securing API Communication including the Open API/Swagger Integration.
41	If required, the proposed solution should have the provision to support comprehensive API discovery, encompassing both known and previously unknown APIs. This includes the ability to learn and understand endpoint structures such as headers, query parameters, supported methods, paths, and request/response bodies and should discover the API schema of applications based on transaction analysis Endpoints, their path parameters, query args, and JSON body params (for requests), identify format definition, such as: integer, string, regular expression, array, complex parameters. This capability should be made available as an optional enhancement, which can be enabled based on specific business needs.
42	The Proposed solution must have SIEM integration capability.
43	The OEM must offer managed services for the solution which helps for fine-tuning, policy review, monitoring, alerting, and troubleshooting. There should not be any restriction or additional cost for creating the security rules. And there must be designated Customer Success Manager who shall also enable Priority service-case handling.

44	The solution must provide a real-time single management console to manage multiple websites. The dashboard must have below widgets as part of Repository : • Access Control Violations • Application Attack Distribution • Application Attack Geomap • Application Security Events • Blocked Geographies Map • Bot Action • Bot Activity Map • Bot CAPTCHA • Bot Classification • Bot Manager Summary • Bot Traffic • DDoS Traffic • HTTP Traffic Volume • HTTP Transactions • Top Application Attack Sources • Top Application Attacked Hosts • Top Attacked Applications • Top Bot Manager Attacks • Top DDoS Attack Sources • Top DDoS Attack Vectors • Top DDoS Attacked Destinations • WAAP Summary
45	The Solution should support role based access control for management and monitoring.
46	The solution must enforce Two Factor Authentication for registered users
47	The Proposed OEM's should be able to support below management features if needed: • Emergency hotline service with up to 10 minutes response time. • On-demand emergency response attack mitigation. • Proactive automatic security anomaly alerts. • Designated Customer Success Manager (CSM). • Post-attack Analysis • Periodic security-status reporting • Priority service-case handling • Security Configuration Review • Chat Support • Policy tuning and configuration management • Annual Attack Test (DDoS L3-7) • External Monitoring on All Apps.
48	The solution should have the provision to export of Access Logs to AWS S3, Azure Storage and SFTP
49	The service shall have continuous asset-health monitoring for on-boarded applications origin server based on TCP and HTTPS. The dashboard should also provide visibility for Origin Response Latency Time.

50	The PoPs/Data Centers shall be fully compliant with all the requirements of the following security-related standards and certificates showing compliances (Valid at all times) against these standards shall be shared along with bid and on demand during contract period: 1. ISO 27001:2022 (Information Security Management Systems) 2. ISO 27017:2015 (Information Security for Cloud Services) 3. ISO 27018:2019 (Information Security Protection of Personally identifiable information (PII) in public clouds) 4. ISO 27032:2012 (Security Techniques -- Guidelines for Cybersecurity) 5. ISO 28000:2022 (Specification for Security Management Systems for the Supply Chain) 6. PCI-DSS 4.0(Payment Card Industry Data Security Standard) Compliant 7. US SSAE16 SOC-1Type II 8. Service Organization Control (SOC) 2- Type II 9. Should be HIPPA Certified
51	Proposed OEM should be able to give atleast 50 threat intelligence queries per months and should have provision to scale up in future.
52	The Threat Intelligence services should features a separate search window within the Unified Portal that lets users investigate suspicious IP addresses and determine their legitimacy. The research results rely on large, diverse data sets to correlate the real-life data gathered from diverse sources in real-time for Open Proxies and Malware Data, IP Insights, malicious activity over-time, identifying source data based on country,IP Type, Proxy, Botnet Member,ASN, CIDR along with types of verticals targeted by Malicious IP addresses.
53	Should have at least 50+ CWAF PoP's globally and PoP level redundancy should be available within INDIA.
54	The Proposed OEM should not be hosted on Hyperscalers like AWS,Azure,GCP,OCI etc. and extend that as a service.
55	The Proposed OEM should be deployed in atleast 3 Govt/PSU organizations.

4. Unified End-point Management

Sl No	Unique Platform Features
1	Uniquely integrated from asset visibility, and vulnerability detection, prioritization to remediation all in one console
2	Interactive Unified dashboard providing a 360-degree view of security posture, asset geo-locations, associated risks, compliance status, and cyber hygiene score.
3	Detect vulnerability and beyond: misconfigurations, asset exposures, security patches, security controls deviation, and posture anomaly
4	Patching and beyond: apply fixes to eliminate all kinds of vulnerability
5	Real-time data analysis, and correlation at the platform for instant visibility and control
6	Real-time communication to any device, located anywhere
7	Continuously updated security intelligence, the industry's best
8	Multi-functional agent to unify cyber security prevention goals
9	Bigdata architecture for speed, scalability, high volume data analysis
10	Multi-tenant, multi-user system
11	Single Sign-on, Multi-Factor Authentication
12	Role-based access control
13	Integration with Active Directory and Microsoft Entra ID (Azure Active Directory) for replicating organizational hierarchy
14	Device discovery with periodic automated scans, port/service/state detection, and advanced name/OS lookup
15	Cater to both SaaS and on-premises deployment requirements

16	Get Visibility from 198 probes and get to know 1470 attributes on your environment
17	1Apply 100s of responses to fix issues
18	Support for air-gapped networks
19	Deployment scalability to achieve millions of devices
20	Onboarding in under 30 minutes
21	Multiple modes of agent deployment
22	Distributed and hub & spoke model for network scanning utilizing agents to perform discovery and vulnerability scanning
23	Agent based, and agent-less scanning
24	Scale up your deployment on-demand and as you go
25	Seamless multi-platform support, covering 30+ operating systems
26	Device tagging with all the pre-discovered tags
27	Add 100s of additional tags for devices and perform tag based operations across tools
28	Import/export of device information in CMDB schema
29	Unlimited scanning, and scanners
30	Enrich organization's CMDB database with device discovery
	Risk Scoring
1	Cyber Hygiene score to quantify risk posture across the organization's IT infrastructure
2	Cyber Hygiene score for individual device, site level and the organization score
3	Cyber Hygiene score to include vulnerability, misconfigurations, missing security patches, posture anomalies and prioritized risks
4	Top risk exposures that contribute to score
5	Top devices that contribute to risk score
6	Prediction and machine learning based score computation to demonstrate trending and possible remediation cycle
	Asset Exposure
1	Continuous device discovery, identify managed and unmanaged assets
2	Categorization of devices by their type, manufacturer, device family
3	Detailed asset inventory, hardware, and software application details
4	Get up-to-date information about devices, services, processes, and open ports
5	Advanced Search Query– Search for Applications, Devices, Services, Processes, and Ports across all devices in the site for comprehensive asset visibility.
6	Discover Shadow IT
7	Software license tracking, uncover under-utilized licenses
8	Discover End of Life, and End of Support Software
9	Discover unused software or rarely used software for effective asset utilization
10	Presence of Blacklisted or unauthorized applications
11	Built Reports & Alerts
	Vulnerability Management
1	Continuous, automated scanning for vulnerability, in five minutes
2	Continuous visibility of IT infrastructure

3	Scan from a database of over 190,000+ vulnerability checks, updated daily
4	Achieve 100% detection accuracy, near-zero false positives
5	Scan network devices, endpoints, servers, cloud workload
6	Configure automated scans by a group of devices
7	Scan by individual IP, range of IP, or multiple subnets by a single network scanner
8	Agent-based, agent-less and network scanner-based detection
9	Always-on vulnerability posture assessment
10	Daily updated security intelligence feed for timely detection
11	Vulnerability insight and risk analysis for each vulnerability
12	Critical rating and grouping for all vulnerability
13	Map vulnerability to high-fidelity attacks, and malware to prioritize remediation
14	Understand vulnerability exploitability
15	Know how to mitigate each vulnerability and prioritize remediation
16	Discover vulnerability beyond CVE using a homegrown vulnerability database
17	100's of dashboard APIs to build visibility to vulnerability
18	Distributed network scanning to efficiently use network bandwidth and system resources
19	Designate endpoint devices to perform network scanning
20	Organize assets to replicate the structure of the business: Sites, Groups
21	Control scan schedule, performance parameters
22	Trending of vulnerability to track over a period
23	Scan external network perimeter and internal scanning with a single solution
24	Scan assets behind the firewall and outside the perimeter
25	Configure Vulnerability Exclusion Policy to exempt specific vulnerabilities from remediation based on accepted risk criteria for a defined period.
26	Receive security alerts from the security research team, high profile vulnerabilities, attacks, patch Tuesday, etc
27	Cloud-native scanning for perimeter-less world
28	Export dashboard elements for reporting
29	100s of reporting APIs to create custom visibility
30	Integrate with other security tools accessing vulnerability findings through REST API
31	Proof of detection for every discovered vulnerability with intuitive depiction
	Patch Management
1	Get alerts on take immediate actions on devices
2	Discover missing security and non-security OS (Windows, Linux, Mac, and AIX) and third-party applications patches
3	Continuous, automated scanning for missing security and nonsecurity patches, in under five minutes
4	Discover open vulnerabilities and patches that can remediate the vulnerability
5	Patch Windows, Linux, macOS, and IBM AIX systems within a single unified console
6	Patch array of third-party software applications, databases, and servers
7	Single click window to fix all critical vulnerabilities based on vulnerability severity, emergency patching based on high-profile exploitable vulnerability

8	Create single patching task to remediate security, non-security and feature update patches.
9	Create, manage, and monitor patching tasks across the organization, with flexibility to patch at the organization or site(s) level.
10	Enable role-based or Job-level patch approval before deployment to ensure governance and control over remediation. Retain previous versions of approved patches.
11	Timely patch availability to accelerate patching activity
12	Searching based on CVE and other security exploitability indexes to mitigate the vulnerability.
13	Always ready to patch compliance report
14	Categorize patches based on their severity to prioritize patching activity
15	Configure automated scans by a group of devices
16	Cloud-based solution for easy and remote patching for all devices
17	Report on device and asset patch compliance, by groups, sites, and across the organization
18	Set patch compliance goals and rollout patches
19	Define & enforce remediation SLAs for different patch categories to ensure timely vulnerability resolution, with real-time compliance reports
20	Measure patching impact gaining knowledge of what vulnerabilities will be fixed and are fixed
21	Apply firmware/device driver patches to fix a vulnerability
22	Rollback already applied patches in case of failure
23	Create automation rules to patch systems without manual interventions, zero-touch patching with control over patch severity and patch type (Security, non-security, feature updates)
24	Pause and Resume of automation rule(s) with a single click
25	Apply patches to a controlled group of devices
26	Test patches and deploy to the production environment through inbuilt workflow for both Manual and Automation jobs
27	Approval workflow between test and deploy phases for manual jobs to provide added control before deploying in production
28	Customize remediation procedure with script execution, prior and post installation of patches
29	Apply patches through custom scripts with configurable inputs
30	Schedule patching with multiple controls, on-demand, repeatable schedules, and time-bound jobs
31	Centralized time scheduling for jobs and automation with option to run at global time or endpoint local time
32	Control & manage device reboots, integrated through patching jobs
33	Get visibility to devices if they are online or offline
34	Deliver messages to end users about patching activity
35	Configure Job Summary Notifications with configurable schedule
36	Specify the remediation time window
37	Monitor patching activities through real-time patching job updates
38	Understand 14 different patching statuses, apart from success/failure
39	Configure Patch exclusion policy to exempt specific patches from remediation based on accepted risk criteria for a defined period.
40	Export dashboard elements for reporting
41	100s of reporting APIs to create custom visibility

42	Demonstrate patching activity and patch compliance
43	Achieve seamless patching within or outside the network perimeter
44	Seamlessly switch patch repository based on the device location
45	Trending of patches to track patching activity over a period
	Endpoint Security Controls Management
	A. Visibility
1	Endpoint Visibility checks, get instant visibility to endpoint activities with 100's bulletin checks
2	Track anti-virus status, running, updated, and if protection is enabled
3	Track system event logs
4	Sensitive data discovery
5	Remote system health monitoring
6	Gain visibility to networks, subnets, and network settings
7	Schedule visibility alerts based on event occurrence
	B. Controls Beyond Patching
1	Multi-platform endpoint management supporting Windows, Linux, macOS, and IBM AIX
2	Software deployment and inventory management covering applications for Windows, Linux, macOS, and IBM A
3	Track and uninstall unwanted software applications
4	Upload custom applications and deploy
5	Deploy software applications silently and with additional command line options
6	Provision installation rules to ensure systems have only authorized applications
7	Block unwanted applications from running based on individual systems or groups of devices
8	Block access to system devices based on individual systems or group of devices
9	Stop or start services and processes
10	System Tune-up to clean unwanted files, registry, browsing history, and download locations
11	Apply network settings across a group of devices
12	Quarantine or isolate a system to a separate network
13	Execute custom scripts
14	Edit system registry, kernel settings
15	Schedule and edit start-up programs, cron jobs
16	Apply security settings, kernel parameters, firewall settings
17	Reboot or shutdown systems
18	Perform file operations from search, edit, to delete
19	Remote system health monitoring
20	Schedule jobs to run periodically
21	Unattended Remote access
22	Remote Access: Multi-user session
23	Remote Shell access
24	Remote file transfer

25	Remote Access: Location independent access, access from anywhere
26	Remote Access: Support for Windows, Linux, Mac
27	Remote Access: Enterprise grade security
28	Remote Access: Keyboard shortcut
29	Remote Scripting: Cross-platform support for Windows, Linux, macOS, and AIX
30	Remote Scripting: Built-in script editor with support for multiple scripting languages
31	Remote Scripting: Schedule one-time or recurring execution of scripts
32	Remote Scripting: Role-based approval workflow for secure execution
33	Remote Scripting: Version control to manage and track script changes
34	Remote Scripting: Central script library for reusable automation tasks
35	Remote Scripting: Audit trails for every script execution
	C. Device Management
1	List of all devices, both managed and unmanaged
2	Track and report unmanaged devices separately
3	Search devices by various filters, hostname, IP, Mac, OS, Group
4	Track device status
5	Group devices based on different criteria: IP, OS, family, device type, and string operations
6	Add devices through an in-built device scanner
7	Deploy agents using multiple deployment methods
8	Configure devices with settings that are applied per group to control the behavior of the agents
9	Delete, and disable unwanted devices
10	Run manual scans by device or group of devices
11	Uninstall agents by device or group of devices
12	Move devices across organizations and sites
13	Create and assign tags to devices for filtering in jobs, rules, and reports
	Reports and Alerts
1	Organization-wide risk assessment report covering all types of risk exposures across the organization and at the site level
2	Organization-wide risk prioritization report covering top prioritized risks by vulnerabilities, misconfigurations, devices, assets and sites across
3	Patching impact reports across the organization and at the site level
4	Canned reports for all modules
5	Generate industry benchmark reports
6	Generate reports for regulatory compliance needs
7	Schedule reports for backup and mail report in PDF format
8	Export reports to PDF, CSV
9	Create different custom reports based on different stakeholder needs
10	1000s of Report API for custom report generation
11	Schedule e-mail-based alerts for 100s of events
	Auditing

1	Track all user activities
2	Export all activities into a CSV for reporting
3	Advance search filters for quick access

5. Multi Factor Authentication & Single Sign On

I	**General Specifications**
1	The proposed solution must be a "Make in India Class 1" Product.
2	The code base must be the same for cloud and on-prem deployments for easy migration in the future.
3	The OEM must have cloud hosting available in India as the organisation may like to partly or fully transition from on-prem to partly or fully cloud environment in the future.
4	The OEM must have large product support capabilities & at least one support center based out of India.
6	The OEM must have implemented IAM in at least 2 customers with more than 20,000 users in India.
7	The OEM must demonstrate strong innovation capability by providing examples, eg: having atleast 1 internationally recognized patent or innovative features developed.
8	The OEM must possess atleast 8 years of experience in the IAM domain.
10	The OEM must participate actively in achieving major implementation milestones.
11	There must be an SME deployed by the OEM to ensure successful implementations.
12	The OEM must demonstrate atleast 1 reference customer of successful implementation of IAM.
13	If necessary, the OEM must be ready to provide a permanent team member to implementation & managed services teams.
II	**Converged IAM Platform**
14	The SSO solution must have capabilities to extend to converged IAM capabilities, including Access Management (AM), Identity Governance and Administration (IGA), and Privileged Identity & Access Management (PIAM), with all IAM modules (AM, IGA, PIAM) present in a single code base, providing a unified administration interface for IGA, PIAM, and Access Management functionalities, managing all IDAM use cases and tasks from a single dashboard or interface, and offering a comprehensive IAM framework encompassing IGA, PIAM, and AM functionalities.
15	The solution must allow the organization to expand the solution to other IAM modules without additional installation.
16	The solution must provide a centralized identity platform (Universal Identity directory) to view, manage & administer all types of user identities in the organization.
17	The solution must easily integrate with existing enterprise systems (e.g., HR systems, security infrastructure, third-party cloud services) as a Source of Truth (SoT) system to collect User Identity information into the centralized identity platform.
18	The authentication flow in the proposed solution must be customizable based on the Organization's business rules/policies.
19	The solution must have a single portal for end-users to perform all kinds of IAM-related activities, such as Access Management (AM), Self-Service Password Management (SSPM), Single Sign-On (SSO), Access Review, Access Request, and Privileged Identity & Access Management (PIAM).
20	The solution must be able to manage all IAM administrative activities such as managing authentication & access policies, on-boarding applications, etc. from the single admin portal.

21	The solution must have a single source code. It mustn't be different modules integrated into one single dashboard.
22	The solution must support multiple authentication sources.
III	**Universal Directory Service**
23	The solution must have a central identity manager to provide real-time visibility into all identity and access-related activities across the organization.
24	The solution must integrate with existing on-premises directory services such as Active Directory (AD) or LDAP.
25	The solution must support the onboarding of various types of users such as employees, vendors, and contractors.
26	The solution must provide APIs for extending directory services and integrating with ERP and other applications.
27	The solution must support bulk or batch importing for identity provisioning.
28	The solution must support different authentication policies for different sets of users.
29	The solutions must have the out-of-the-box connector built for various SoT systems and applications.
30	The solution must provide a self-service portal for end-users to manage their profiles and credentials, and perform various IAM activities.
IV	**Single Sign On & MFA**
31	The solution must act as the centralized authentication gateway for application access for all types of users.
32	The solution must support standard protocols like SAML, WS-Federation, OpenID Connect, and OAuth 2.0 for integration with various applications for authentication and authorization.
33	The solution must include SSO for thick-client and thin clients-on MS Windows.
34	The solution must support standard authentication protocols such as OAuth 2.0, API keys, or JWT (JSON Web Tokens) for non-federated applications.
35	The solution must restrict any direct access to non-federated web applications.
36	The solution must support cross-browser support for web or federated applications.
37	The solution must support native-device authentication factors.
38	The solution must provide APIs to enable single sign-on for internal applications and target systems.
39	The solution must support Password less Authentication. (Leverage native device authentication factors or Out-of-band Authentication with a Mobile Application)
40	The solution must support out-of-the-box authentication factors such as Email OTP, SMS OTP, Soft-token etc.
41	The solution must support password less Authentication as an MFA for Core Banking Applications.
V	**Audit, Compliance, and Reporting**
42	The solution must provide comprehensive audit reports that include both successful and failed access attempts.
43	The solution must allow for user login reports to be exported in CSV, PDF, or Excel formats.
44	The solution must support customized reports as per organizations requirements
45	The solution must maintain detailed event logs
46	The solution must have the user login reports which include detailed information like user ID, timestamp, and login success or failure.
47	The solution must integrate with SIEM tool

6. Vulnerability Management

Sl.No.	**Requirement**
1	VA (Vulnerability Assessment) software License for scanning of IPs
2	The Solution should be on-premises with no dependency on the cloud except for vulnerability signature, DB updates and should not rely on component/service hosted outside the Organization's premises for any feature functionality or product capability. It should cater to perform vulnerability scan of all IP devices present in the environment.
3	The Software should identify vulnerabilities such as software flaws, missing security patches, threats like malware, and misconfigurations, across a variety of operating systems, devices, and applications.
4	The Software should automatically update in real-time
5	The tool provides should have Custom plugins to create specific checks to assess the security of applications unique to the organization
6	The tool should provide vulnerability rating
7	There should be no limit to the number of IPs or assessments
8	The tool should easily customize reports with client name and logo
9	The solution should Email directly to the client after every assessment
10	The solution should have Out-of-the-box, pre-configured templates for IT and mobile assets, including configuration audits
11	The tool should be scalable for small to large enterprise environments with distributed scanning capabilities.
12	Discovery: Accurate, high-speed asset discovery • Scanning: Vulnerability scanning (including IPv4/IPv6/hybrid networks) • Un-credentialed vulnerability discovery • Credentialed scanning for system hardening and missing patches • Meets PCI DSS requirements for internal vulnerability scanning • Coverage: Broad asset coverage and profiling • Network devices: firewalls/routers/switches/servers/desktop/laptop/storage • Offline configuration auditing of network devices
13	Flexible reporting: Customize reports to sort by vulnerability or host, create an executive summary or compare scan results to highlight changes.
14	Generate compliance-focused reports with specific guidelines and controls for regulatory standards.
15	provides extensive coverage across various environments, ensuring robust security and vulnerability management
16	Provides active scanning, agents, passive monitoring, and CMDB integrations to gain the visibility you need to reveal impactful vulnerabilities across your environment
17	Provides a deeper understanding and context of your assets by assigning criticality ratings, helping prioritize remediation efforts based on asset importance
18	Take rapid, decisive action with Predictive Prioritization technology–with vulnerability data, threat intelligence and data science–to close critical exposures and execute remediations.

19	Measures the exposure of assets to vulnerabilities, providing a clear metric to assess and manage risk
20	Continuously monitors and discovers assets and vulnerabilities in real-time, ensuring the highest level of visibility and Security
21	The System should Create reports based on customized views (e.g., specific vulnerability types, vulnerabilities by host/plugin, by team/client) – in a variety of formats (HTML, CSV / PDF).
22	Vendor has to provide documentation, literature of the version of the software supplied stating system requirements, etc.
23	Vendor recognized as a leader in the vulnerability management market with extensive coverage and significant market share.
24	Vendor provides rich context on vulnerabilities, including the likelihood of exploitation and potential impact.
25	Vendor offers 250 pre-built integrations to streamline processes.
26	Vendor provides advanced vulnerability intelligence features to stay ahead of potential threats.
27	Vendor ensures superseded patches technology, replacing outdated patches with the latest ones.
28	Vendor provides access to a vast database of vulnerabilities sourced from internal expertise, vendor advisories,and the National Vulnerability Database (NVD).
29	Vendor blends known risk indicators with insights to highlight the most critical vulnerabilities.
30	Vendor allows users to search vulnerability database, view detailed vulnerability profiles, and identify exposure compared to known vulnerabilities.
31	Vendor helps prioritize remediation efforts by comparing identified vulnerabilities with your own findings and building actionable lists.
32	Vendor provides timelines for each CVE to support informed decision-making, asset protection, and accelerated incident response.
33	Vendor offers the most extensive plugin coverage to ensure comprehensive vulnerability detection and management.
34	Vendor provides insights on Asset Criticality, Asset Exposure, prioritize actions
35	Vendor maintains a data lake of data points
36	Vendor maintains approximately 190,000 plugins, detections, and policies, with around 40,000 unique audit checks.
37	Vendor ensures new detections are added within a 24-hour cycle, keeping the system up-to-date with the latest threats.
38	Vendor is supported by the largest research team, working 24/7 to deep dive and update continuously, ensuring comprehensive coverage.

7. End point Detection & Response

Sno.	Technical Features
1	Must offer comprehensive client/server security by protecting enterprise networks from viruses, Trojans, worms, hackers, and network viruses, plus spyware and mixed threat attacks.
2	Must be able to mitigate or stop the risk of virus/malware entering the network by blocking files with real-time compressed executable files.
3	Must include capabilities for detecting and removing rootkits

4	Must provide Real-time spyware/gray ware scanning for file system to prevent or stop spyware execution
5	Must have capabilities to restore spyware/gray ware if the spyware/gray ware is deemed safe
6	The proposed solution should have but not limited to the following prevention capabilities: • Antimalware with signature/Pattern based detection • Ransomware protection • Machine learning - pre-execution and runtime • Browser exploit protection • Behavior monitoring • Injection protection • Script protection • Anti-exploit • C&C communication prevention • Application control • File less malware prevention • File/web reputation
7	The solution should offer a combination of signature-based malware protection, behavioral analysis, and AI/machine-learning based analysis.
8	Must provide Outbreak Prevention to limit/deny access to specific shared folders, block ports, and deny write access to specified files and folders on selected clients in case there is an outbreak.
9	Must clean computers of file-based and network viruses plus virus and worm remnants (Trojans, registry entries, viral files)—through a fully-automated process
10	To address the threats and nuisances posed by Trojans, the solution should be able to do the following: Terminating all known virus processes and threads in memory,Repairing the registry,Deleting any drop files created by viruses,Removing any Microsoft Windows services created by viruses,Restoring all files damaged by viruses,Includes Cleanup for Spyware, Adware etc.
11	The solution must have behavior monitoring module to constantly monitor endpoints for unusual modifications to the operating systems or on installed software's to provide additional threat protection from programs that exhibit malicious behavior.
12	Behavior monitoring should restrict system behavior, keeping security-related processes always up and running, able to block ransomware activity by killing such processes,enable Certified Safe Software Service to reduce the likelihood of false positive detections
13	The solution must be able to create copies of files being encrypted by a ransomware on the endpoint and it must be able to restore the affected files back to their original state.
14	The solution must have an integrated Application Control module to enhance defenses against malware and targeted attacks by preventing unknown and unwanted applications from executing on corporate endpoints with a combination of flexible, dynamic policies, whitelisting (default-deny) and lockdown capabilities(llow or prevent users from changing settings or unloading/uninstalling the software).

15	The proposed solution should support SHA1 & SHA2 Hash values to be imported and block/allow the same from executing. Solution must support importing inventory of hashes to define a Application control criteria.
16	Shall support grouping of clients into domains for easier administration
17	Establish separate configuration for internally versus externally located machines (Policy action based on location awareness).
18	Shall be able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other) and Malware type (Adware, Spyware, Ransomware etc.).
19	Shall be able to scan only those file types which are potential virus carriers (based on true file type).
20	Should be able to detect files packed using real-time compression algorithms as executable files.
21	Shall be able to scan Object Linking and Embedding (OLE) File.
22	Must provide a secure Web-based management console to give administrators transparent access to all clients and servers on the network.
23	The management server should be able to download updates from different source if required, which could be the vendor's update server, any other server or a UNC path.
24	If the update from the Management server fails, the security clients with privilege should be update directly from the vendor's server/Cloud.
25	Must reduce network traffic generated when downloading the latest pattern by downloading only incremental patterns.
26	Must have the flexibility to roll back the Virus Pattern and Virus Scan Engine if required via the web console.
27	Should have role-based administration with active directory integration: To create custom role type,To add uses to a predefined role or to a custom role.
28	Must be capable of uninstalling and replacing existing client antivirus software automatically
29	The solution must support legacy and rare operating systems including but not limited to the below mentioned operating system:
	a. Microsoft Windows 10,11, Windows Server 2012 & 2012 R2, 2016,2019, 2022
	b. RHEL 6,7,8 ,9
	c. CentOS 6,7,8
	d. Ubuntu 16,18,20 & 22
	e. Debian 8,9,10 & 11
	f. Solaris 10.0,11.0,11.1,11.2,11.3,11.4
	g. Oracle Linux 6,7,8,9
	h. AIX 6.1,7.1,7.2 & 7.3
	i. SUSE Linux 12,15
	j. MacOS BigSur, Monterey, Ventura, Sonoma, Sequoia
30	Must be able to send notifications whenever it detects a security risk on any client or during a security risk outbreak, via email.
31	Must be able to send a customized notification message to specified recipients when firewall violations exceed certain thresholds, which may signal an attack.

32	The solution allows creating rules to filter connections by application, IP address, port number, or protocol, and then apply the rules to different groups of users.
33	Must support both Pre-execution and Run time execution mode in the Machine-learning module to support noise cancellation, which reduces false positives.
34	The solution should support off-premise security for the end-point.
35	The solution should support CPU usage performance control during scanning: adjust the scanning speed, if the CPU usage medium or low and actual CPU usage exceeds certain threshold.
36	Should be able to provide in a single agent the following features: Anti-malware, Behavioral Monitoring, Application Control, Device Control, Extended detection and response from day one.
37	Must have a host-based intrusion prevention system (HIPS) to virtually patch known and unknown vulnerabilities before a patch is available or deployable.
38	The solution must have an Vulnerability Protection feature which can not only give visibility on vulnerabilities but it should also have rules to virtually patch those vulnerabilities targeting endpoint OS using Deep Packet Inspection and assign CVE ID, CVSS score mapping to the rules to reduce risk exposure due to missing patches.
39	Solution shall shield endpoints from network exploitable vulnerabilities targetting endpoint OS
40	Solution should be able to block malicious uploads to SMB share and must be able to detect and block remote powershell
41	The proposed solution should support SHA1 & SHA2 Hash values to be imported and block/allow the same from executing
42	Solution should support to use application name, path, hash or category for basic application whitelisting and blacklisting.
43	The proposed solution must support Device control - Whitelisting/Blacking listing of devices.
44	The solution must support to configure advance access permission -Full Access, Read only, Execute, Modify
45	The solution must support Network Devices, USB, Mobile Storage, Non-Storage devices, Bluetooth adapter, Com/LPT, Imaging, Prt Screen key ,Wireless Nic
46	Should include predefined detection models which combine multiple rules, and filters using techniques such as machine learning and data stacking. Should be regularly updated to improve threat detection capabilities and reduce false positive alerts.
47	The solution should be able to analyze and determine if certain indicators signal an ongoing attack, enabling SOC team to take timely prevention, investigation, and mitigation actions against targeted attack campaigns.
48	Should provide more context with mapping to the MITRE ATT&CK TTPs for faster detection and higher fidelity alerts.
49	The solution deployment model must support to air-gapped, onpremises, and hybrid deployments.
50	The proposed solution should provide on-premises virtual server component which will be hosted at the customer data centre in a forward proxy mode for any communication between endpoints and the OEM's EDR solution.

51	Should have the capability to write custom search queries, add the saved queries to the watchlist, and automatically execute them against the latest telemetry data on an interval basis.
52	Should have the capability to write custom search queries, add the saved queries to the watchlist, and automatically execute them against the latest telemetry data on an interval basis.
53	The solution should have an AI-powered chatbot to guide with the investigations and automatically provide answer to any questions related to cybersecurity.
54	Generate a root cause analysis, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets.
55	The console should provide different search methods, filters, and an easy-to-use Kibana-like query language to identify, categorize, and retrieve search results.
56	Add or Remove indicators of compromise to block list including but not limited to File hash, URL, IP address, and Domains.
57	The solution should allow a SOC analyst to manually add IoCs such as File Hashes, IP Addresses, Domains, and URL's as part of the custom intelligence.
58	The solution should allow you to perform sweeps identifying indicators of compromise (IoC) and indicators of attack (IoA).
59	Automatic and manual collection of forensic evidence from specified endpoints and upload the forensic package back to the management console for further investigation.
60	The solution must support automatic and manual sweeping based on vendor curated and third-party custom intelligence to search your environment for indicators of compromise.
61	Remotely connect to an endpoint and dump process memory.
62	Ability to remotely connect and execute custom PowerShell or Bash scripts.
63	Ability to execute custom YARA rules on the specified endpoints.
64	Ability to view and terminate active processes on a specific endpoint or multiple endpoints.
65	The solution should provide a unified platform that enables security teams to take immediate response and track actions for both servers and endpoints from single console
66	The solution should provide a platform for easier investigation like visual graphical view and timeline of the attack.
67	The solution should have the capability to automate a variety of actions using Security Playbooks to help reduce workload and speed up security tasks and investigations.
68	The solution needs to include an ability to build security playbooks against threats and risks, such a blocking the activity of a file, shutting down an endpoint, disconnecting an endpoint from the internet, entering files into quarantine, deleting malicious files and etc.
69	Provides insights into the organization's security posture using an Executive level dashboard. Must be able show the company's overall risk score, individual asset risks, a view of ongoing attacks and its contributing risk factors.

70	The solution should be able to produce manual and scheduled reports that can be customized to display company information and logo. Generated reports should at least support PDF/PPT format and can be sent to specified email recipients.
71	The solution should provide a unified platform that enables security teams to run a root cause analysis, investigate the execution profile of an attack, and identify the scope of impact across assets.
72	The solution should provide 30 days raw data retention by default and retain threat alerts/workbenches for 180 days to give information for investigation/reporting.
73	The solution must have participated with strong performance and impressive results in MITRE Engenuity ATT&CK® Evaluations
74	The proposed OEM should have a connected threat defense ecosystem with protection, detection and response capabilities to proactively protect endpoints, hybrid cloud, and network environment and to share IOC's amongst above protection layers by leveraging collective threat intelligence
75	The proposed solution should have flexible deployment options including on-premises, cloud, and hybrid deployment capabilities to suit customer requirements
76	The proposed OEM should have data center and data lake in India to adhere to data localisation guidelines
77	The proposed OEM should have a support center present in India to provide quick assistance and improve customer satisfaction

8. Run time Application Self Protection

S. No.	**Specifications of required Capabilities**
1	Mobile App Security SDK to prevent the mobile app from running on Emulators & Simulators
2	Mobile App Security SDK to detect if the mobile app is running on a Jailbroken (for iOS) or Rooted (for Android) device
3	Mobile App Security SDK to detect Elevation of Privileges by the attacker
4	Mobile App Security SDK to detect if the mobile app is running on an outdated operating system
5	Mobile App Security SDK to identify if an android device has third party app store access enabled
6	Mobile App Security SDK to detect if USB Debugging Mode and/or Developer Options are enabled on the android device
7	Mobile App Security SDK to detect Hooking Frameworks on Devices
8	Mobile App Security SDK to detect Device Screen Lock enablement
9	Mobile App Security SDK to enforce Device Policy as per business needs
10	Mobile App Security SDK to detect if the mobile app is running in a Sandbox environment
11	Mobile App Security SDK to detect if the mobile app is launched with the secondary profile on the Android device
12	Mobile App Security SDK to detect if mock location settings are enabled on the device

13	Mobile App Security SDK to detect time manipulation settings on the device
14	Mobile App Security SDK to prevent keystroke recording by malicious apps or keyloggers
15	Mobile App Security SDK to detect code injection attempts within the mobile application
16	Mobile App Security SDK to implement behavioral-based blacklisting of malicious devices
17	Mobile App Security SDK to detect if the mobile app is running on an unsecure Wi-Fi network
18	Mobile App Security SDK to identify a Rogue Access Point (RAP) when it is connected to the device
19	Mobile App Security SDK to detect MiTM attacks
20	Mobile App Security SDK to monitor and prevent SSL Stripping
21	Mobile App Security SDK to detect fake certificates used for SSL decryption
22	Network threat detection function should be able to work without internet connectivity to app hosting servers
23	Mobile App Security SDK to detect Proxy & VPN connections
24	Mobile App Security SDK to allow IP whitelisting for trusted VPN connections
25	Mobile App Security SDK to detect and defend against offline attacks by identifying when the device has no internet connection
26	Mobile App Security SDK to prevent reverse engineering of the mobile app
27	Mobile App Security SDK to detect if the mobile app is being tampered
28	Mobile App Security SDK to prevent the attackers from decoding or modifying the business logic
29	Mobile App Security SDK to detect runtime recompilation or modification of an application
30	Mobile App Security SDK to detect if the App is not downloaded from trusted source - Play store and App Store
31	Mobile App Security SDK to detect if the App is in Debug Mode
32	Mobile App Security SDK to detect if any blacklisted application is present on the mobile device
33	Mobile App Security SDK to prevent Screen shot capturing
34	Mobile App Security SDK to prevent APK file Decompilation
35	Mobile App Security SDK to detect active screen mirroring during App usage
36	Mobile App Security SDK to detect App Spoofing Attacks when the App is launched
37	Mobile App Security SDK to detect side loading when the mobile app is launched
38	Mobile App Security SDK should not collect any personal information from customer devices while protecting the Mobile App from malware. Therefore, malware protection should be based on behaviour methodology and not on signature methodology
39	Mobile App Security SDK to identify any overlay during App usage
40	Mobile App Security SDK should work all the time as long as App is alive and active to protect from Malware threats, not just on the launch of the App
41	Mobile App Security SDK to prevent Picture-in-Picture (PIP) Attacks and Draw over other App
42	Mobile App Security SDK to identify Admin & Accessibility permission for Sideloaded Apps

43	Mobile App Security SDK should comply with OWASP Mobile Top 10
44	Mobile App Security SDK should support minimum Android version 8 and iOS version 12
45	Mobile App Security SDK should be able to support any device model having minimum Android version 8 or iOS version 12
46	Mobile App Security SDK to notify the host application through callbacks in the event of device, network or malware-based threat detection
47	Mobile App Security SDK should provide the API's to query the security state of the device by additional reference IDs already available with parent App system.
48	Mobile App Security SDK should not collect any PII data from device or app
49	Mobile App Security SDK should be able to allow for the usage of custom device identifiers and labels
50	Mobile App Security SDK should be capable to execute detection of threats even if its System Control Portal is not reachable. Explain your approach on workings of detection and how threat data will be sent to console
51	Mobile App Security SDK to support React Native framework
52	Mobile App Security SDK should provide the means of mapping the threat data detected with the actual user session or user id
53	Mobile App Security SDK should comply with the security policies of Play Store and App Store, etc
54	Management Console Should integrate with SIEM/SOC platforms and provide all detailed threat forensic information
55	Management Console should integrate with Fraud Prevention System
56	Management Console should support Rest API's for integration with backend system
57	Mobile App Security SDK to provide unique ref. or message ID on detection of each threat
58	Mobile App Security SDK should have the capability to collect information of applications and processes running at the time of threat detection
59	The Management Platform should be available on SaaS / On Prem platform.
60	The SaaS solution should have the capability of multi-tenant architecture deployment.
61	The SaaS / On Prem solution should have data localization with DC and DR hosted in India.
62	Management Platform should have option to deploy in High-Availability mode
63	Mobile App RASP solution must be SDK based and there should not be dependency on Service provider for App version upgrades
64	System Control Portal should be a web-based solution for configuration, integration and reporting of Mobile App RASP Solution
65	System Control Portal should provide Role based access to console with proper segregation of group of users and functions.
66	System Control Portal should provide details of No. of devices on which App is running on with breakup of Android and iOS devices.
67	System Control Portal should include details such as device OS version details, OS level threats detected, etc.
68	System Control Portal should provide customizable Threat Policy configuration for different Apps

69	System Control Portal should provide over the air updates for rule upgrades and configuration
70	System Control Portal should provide statistics on Daily, Monthly Active devices
71	System Control Portal should provide Dashboards highlighting change in trend of threats
72	Service Provider should perform Annual App Assessment as per OWASP Mobile Top 10 Guidelines
73	Service Provider should provide quarterly version updates
74	Service provider should assist to close any code related vulnerabilities identified during VAPT or Code Review
75	Service provider should undertake detailed Threat Modelling exercise before implementation of Mobile RASP solution

9. External Attack Surface Management

Sno.	Technical Features
1	Solution should be able to continuously identify, categorize and document all the assets within the organization's digital ecosystem. Assets should be listed and categorized but not limited to the following asset categories: Internet-facing Assets Internal device Assets Account Assets Application Assets Cloud Assets APIs
2	Solution should work natively with the proposed endpoint security solution by taking native response actions without the need for integration with any other solution.
3	Solution should be able to cover the following environment - IT, OT, SaaS and multiple Cloud Infrastructure for asset discovery, asset inventory and risk assessment and prioritization.
4	Solution should provide contextual visibility into all assets by: Criticality based on asset attribute and activity. Graphical presentation on relationship of assets Historical risk assessment result
5	Solution should be able to manage all discovered assets from a single unified management console.
6	Solution should have complete contextual visibility into Cloud Assets. The solution should be capable of continuously prioritizing security risks related to: Compliance Vulnerabilities Security Misconfiguration Threats
7	Solution should be capable of integrating with a cybersecurity platform that can manage the organization's Endpoint, Email, Cloud, Network, OT Security, XDR, and Zero Trust solution from a single console and do informed decision making
8	Solution should be able to integrate with 3rd party vendors for ingest or enrich attack surface data.
9	Solution should be able to integrate with a Zero Trust solution for user account and device assets and be able to trigger zero trust actions from within the management console.
10	Solution should provide an organization wide risk score based on continuous assessment of risks in the organization.
11	Solution should provide an exposure index score that summarizes the likelihood of an exploit or threat to occur in the environment.

12	Solutions should provide an attack index score which summarizes the number of known detections, impacted assets and the severity of each unique threat in the environment.
13	Solution should provide a security configuration index score that summarizes deployed and missing security controls within the environment.
14	Incorporate asset criticality, vulnerabilities, threat activity and configuration of security controls in the calculation of risk score for each asset type.
15	Should be able to list all domains and respective subdomains belonging to the organization and provide domain discovery trend data monthly for at least one year.
16	Should be able to list all Public IP addresses belonging to the organization and provide IP asset discovery trend data monthly over time for at least one year.
17	Should be able to provide the Internet-facing asset's latest risk score, host provider, services, ports and show when the asset was last seen.
18	Provide risk assessment for each domain and IP address asset and assign a risk score that can be monitored over time. Display risk indicators like what type of risks, events, and risk level for each discovered risk.
19	Should be able to show an asset graph for each domain and IP asset. An asset graph graphically illustrates the asset's connection to internal assets in the environment.
20	Provide an asset criticality score per domain and IP asset. Asset criticality indicates the importance of an asset in an organization. Administrators should be able to manually change asset criticality.
21	Should be able to summarize IP address asset's location per country and display on a map view.
22	Ability to add company owned domains, subdomains, and IP addresses for discovery. Manually added IP addresses should be displayed.
23	Can utilize multiple discovery data providers (Reliance to existing agent should be supplemented by additional discovery providers)
24	Should be able to provide the internal device asset's latest risk score, OS, IP address, last user, vulnerabilities, discovery source and when the device was first and last seen.
25	Provide risk assessment for each device asset and assign a risk score that can be monitored over time. Display risk indicators like what type of risks, events and risk level for each discovered risk.
26	Should be able to show an asset graph for each device asset. An asset graph graphically illustrates the asset's connection to other assets in the environment.
27	Provide an asset criticality score per device asset. Asset criticality indicates the importance of an asset in an organization. Administrators should be able to manually change asset criticality.
28	Solution should be able to identify managed and unmanaged devices.
29	Should be able to list all discovered internal device assets and show discovery trend monthly over time for at least one year.
30	Show device asset's cloud application usage and activity
31	Show device asset's use of sanctioned and unsanctioned cloud applications.
32	Show device asset's device activity by displaying device location on map.
33	Show device assets logged on users including username, email address, location, job title and user risk score.
34	Provide an asset criticality score per device asset. Asset criticality indicates the importance of an asset in an organization. Administrators should be able to manually change asset criticality.
35	Provide a summary of a device asset by building an asset profile. Details should include basic device info (OS, device type, group membership, etc), Activity, Device Usage, Connection information, Influence, and Identity posture risk.
36	Perform Response Actions (for ex: Isolate, Remote Shell, Run Custom Script) and Zero Trust Actions (for ex: Block App or Cloud App Access) to device assets.

37	Can utilize multiple discovery data providers (Reliance to existing agent should be supplemented by additional discovery providers)
38	Identify both domain and service accounts.
39	Should be able to provide the account's latest risk score, user type, role, location, job title and when the account was first and last seen.
40	Provide risk assessment for both domain and service accounts and assign a risk score that can be monitored over time. Display risk indicators like what type of risks, events, and risk level for each discovered risk.
41	Should be able to show an asset graph for both domain and service accounts. An asset graph graphically illustrates the asset's connection to other assets in the environment.
42	Provide an account criticality score for both domain and service account. Account criticality indicates the importance of the account in an organization. Administrators should be able to manually change the account criticality rating.
43	Enumerate exposed APIs connected to discovered service accounts.
44	Enumerate application roles granted to discovered service accounts.
45	Enumerate granted consent permissions to discovered service accounts.
46	Should be able to list all discovered accounts and show account discovery trend monthly over time for at least one year.
47	Show account's cloud application usage and activity.
48	Show account's use of sanctioned and unsanctioned cloud applications.
49	Show account's activity by displaying logon data location on map.
50	Show account's latest account risk score, user type, role, location, job title and when the account was first and last seen.
51	Provide a summary of an account by building an asset profile. Details should include basic account info (level, role, group membership, etc), Activity, Device Usage, Email usage information, Influence, and Identity posture risk.
52	Perform Response Actions (for x: Isolate, Remote Shell, Run Custom Script) and Zero Trust Actions (for ex: Block App or Cloud App Access) to device assets.
53	Provides vulnerability management metrics for both internal and Internet facing assets over time and be able to compare the organizations score to the global average. Metric: Highly Exploitable unique CVEs.
54	Provides vulnerability management metrics for both internal and Internet facing assets over time and be able to compare the organizations score to the global average. Metric: Mean Time to Patch
55	Provides vulnerability management metrics for both internal and Internet facing assets over time and be able to compare the organizations score to the global average. Metric: Average Unpatched Time
56	Provides vulnerability management metrics for both internal and Internet facing assets over time and be able to compare the organizations score to the global average. Metric: Vulnerable endpoints
57	Supports automation/playbook actions for vulnerability detection events.
58	Agentless Vulnerability Assessment and Threat Detection - provide a serverless scanned in your cloud account to scan for vulnerabilities without impact to other resources and running applications.
59	Vulnerability Assessment and Prioritization should be based on both external factors (threat intel, e.g. whether a CVE is highly actively exploited) and internal factors (asset criticality, exploit attempts based on detection logs) and security controls (virtual patch via IPS rule)
60	Provide zero-day vulnerability detection capability and virtual patching via IPS rule to mitigate zero-day vulnerability.
61	Automate and orchestrate response actions to mitigate risks and respond to threats using advanced AI and ML technologies.
62	Provide remediation steps for all discovered risk factors
63	Ability to set a goal for risk reduction measures. Provide a way to lower the organization's risk level (ex: high risk to low risk) by offering a list of recommendations.

64	Keep track of discovered risks events by specifying remediation status for every discovered event. Events status should be able to be assigned per event (ex: Remediated, Dismissed etc.).
65	Provides insights into the organization's security posture using an Executive level dashboard. Must be able to show the company's overall risk score, individual asset risks, a view of ongoing attacks and their contributing risk factors.
66	Provides the ability to assess and mitigate vulnerabilities related to users, devices, and device assets on an Operations dashboard.
67	The proposed OEM should have data center and data lake in India to adhere to data localisation guidelines
68	The proposed OEM should have a support center present in India to provide quick assistance and improve customer satisfaction

10. NBAD-NDR

Sr . No	Specifications
1	Proposed NDR Systems should be hardware-based appliances.
2	All systems / sub –systems of proposed NDR systems should have dual redundant hot swappable internal power supply.
3	The proposed solution must support full packet capture/ smart Capture.
4	The solution should be sized for 2 Gbps from day one with ability to scale upto 10 Gbps in future.
5	Bidder is to quote hardware appliances (i.e. Compute, Memory, storage, Operating Systems, DB, replication and corresponding licenses etc). Sizing of hardware and software is to be certified by prospective OEM and certificate from OEM along with bid is to be submitted by Bidder. In case of any shortfall in hardware and software, the OEM will be responsible to supply additional hardware and software without any financial cost to User to ensure successful deployment of the NDR solution. All hardware and software components of appliance-based solutions must be hardened to ensure security of the system and all versions of OS/firmware/patch update schedule/ best practices must be shared by OEM with User.
6	The system should be designed and deployed to work with the existing network and devices and should not require re-architecting the network or replacement of existing devices.
7	Proposed NDR systems should not have any dependency on existing switching infrastructure including but not limited to make, model,IOS, version etc.
8	Responsibility of configuring the switches for successful deployment of proposed NDR systems lies with the bidder at BSES locations as applicable.
	Visibility & Identity
9	The NDR tool should provide the internal network visibility and actionable insight required to quickly identify the threats. Additionally, NDR integrates user information with network traffic statistics to deliver detailed intelligence into user activity anywhere across the network.
10	The Network Detection and Response (NDR) solution should provide extensive flexibility and capability to delve deeply into end-user activities, MAC (Media Access Control) addresses, network flows, interface utilization, and a comprehensive range of other host statistics essential for swift incident resolution. It must leverage anomaly detection

	techniques to detect various types of attacks, including zero-day exploits, self-modifying malware, intrusions.
11	The proposed solution must have the ability to natively monitor layer 7 traffic and perform deep packet inspection (DPI) without any 3rd party solution
12	By collecting, analyzing and storing information from various sources, the NDR System should provide a full audit trail of all network transactions and perform more effective forensic investigations.
	Functional Requirements
13	The solution should be able to provide real-time monitoring and visibility into all network traffic, using machine learning, context-aware analysis, and on-premise threat detection and analytics.
14	Network Detection and Response (NDR) solutions leverage the inherent packet/ flow technologies present in network devices. These tools should possess the capability to capture packets from ongoing streams of real-time network traffic and transform this raw data into actionable analytics represented through numerical data, charts, and tables. This analytical output serves to quantify precisely how the network is utilized, by whom, and for what purposes.
15	The solution should provide contextual network-wide visibility viaan agentless approach.
16	NDR solution should be able to use the existing network environment to analyze traffic across the across the existing network and security solutions in a nondisruptive manner.
17	The solution should have an automated discovery function to identify network devices and capture information such as IP address, OS, services provided, other connected hosts.
18	The system should be able to monitor flow data between various VLANs.
19	The solution should have the capability of application profiling in the system and also support custom applications present or acquired by the end user.
20	The solution should have the capability to enrich flow records with additional fields including source and destination IPs, source and destination MAC address, TCP/UDP ports or ICMP types and codes, number of packets and number of bytes transmitted in a session, timestamps for start and end of session, NAT translations, etc. from captured data and then utilize those fields in analytical algorithms to alarm on anomalous behaviors.
21	The solution must be able to track user's activities locally and remote network sites and should be able to report usage behavior across the entire network.
22	The solution should support all forms of flows including but not limited to Netflow, IPFIX, sFlow, Jflow, cFlowd, NSEL or packet capture based solution.
23	The solution should be able to combine the packet / flow records coming from different network devices like routers, switches, firewalls that are associated with a single conversation

24	The solution must be able to stitch packets/ flows into conversations even when the traffic is NATed by the firewall; clearly showing the original and translated IP address.
25	The solution must provide an application bandwidth utilization graph for various applications which should include bandwidth consumption for top hosts and trends on network bandwidth utilization.
26	The solution must probe the network in a manner so that impact on network performance is minimal.
27	The solution must be an out of band analytics engine from the primary data path.
28	The system should provide detailed visibility to identify asset-based information within the network automatically.
29	The solution should have capability to assign risk and credibility rating to alerts and present critical high-fidelity alerts prioritized based on threat severity with contextual information on the dashboard.
30	The solution should provide use cases to identify usage of insecure, legacy and deprecated encryption algorithms being used by servers on the network.
31	The solution should provide the capability to define custom policies to evaluate flow attributes such as bytes, services, process, name and more.
32	The solution must have the capability to identify network traffic from high risk applications such as file sharing, and perform a continuous evaluation of threat actors, and cluster the behaviour to detect sophisticated attacks.
	Threat Detection Capabilities
33	The NDR solution should provide enterprise-wide network visibility and apply advanced security analytics to detect and respond to threats in real time. NDR solutions must be able to detect threats such as reconnaissance, data hoarding/exfiltration, distributed-denial-of- service (DDoS) attacks and insider threats.
34	The solution should detect significant anomalies and drifts in user, device or network activities and traffic that signal an attack.
35	Detect in-progress attacks as they evolve and a true 360° view in the networks like whom and what is really using your data or facilities.
36	The solution must identify an attack on the corporate network using a RAT (Remote Access Tool) like unknown/known botnets.
37	The solution must detect anomalous data transfer from/to the corporate network or within the network.
38	The solution must detect unusual, unauthorized behavior within the network. This includes but is not restricted to unusual RDP, port
39	Systems can produce detailed visibility to identify the endpoints and its information within the network automatically.
40	System monitors traffic passively without being invasive on the network with the ability to send alerts in real time.
41	System has the capability to historically track the location, dates first/last seen and summary of malicious activity.
42	The solution should perform analysis on network data all the way up to the Layer 7 and provide complete application visibility
43	The solution should be able to detect command and control bot communication based on the domain/url the user is trying to access.
44	The solution should have DNS Threat Analytics Capability to detect the threat present in DNS traffic.
45	The solution should have capability to detect DNS tunnelling.
46	The solution should be able to detect vertical and horizontal scans within the environment

47	The solution should highlight weak ciphers being used in the network by hosts or applications. The solution should search and monitor cipher suites and report on which ones are used on the network.
48	The solution should be able to analyze SMTP traffic to detect high volume email, abnormal patterns in email traffic, traffic from unfriendly countries and with character sets often used by attackers (ex. Chinese).
49	The solution should be capable of rejecting particular network data from analysis using input filters.
50	It should have capability to detect and predict any data exfiltration by identifying abnormal behavior as part of cyber kill chain stages.
51	The solution should support active scanning of specific enterprise assets in addition to passive profiling of devices on the network.
52	Solution should be able to detect and monitor ransomwares and malwares.
53	The solution must support VPN tunnel detection for private and anonymous VPN tunnels and just not the VPN used by the Organization. Privacy VPN - Personal VPN solutions which enable the user to avoid network monitoring solutions.
54	The solution should support extraction of the payloads in the network traffic.
55	The solution must support port-agnostic protocol detection. The solution should be capable of detecting protocols and applications despite them using non-standard TCP/UDP ports.
56	NDR solution should provide a full-featured Network threat analyzer capability to detect threats emerging from inside the network (i.e., ones that have not passed through a perimeter FW/IPS).
57	The NDR solution should be able to get threat intelligence from the research team to make detections of malware activity with higher accuracy and efficacy including Botnets, C&C servers, Bogons, Tor Entry/Exit Nodes, Connections to bad reputation Nations and Dark IPs..
58	The solution must identify worms through techniques such as identifying the use of normally inactive ports or identification of network scanning activities.
59	The solution should detect events of denial-of-service (DoS) with IoCs/ Behavioural (deviation from normal routine traffic) and distributed denialof-service (DDoS) attacks with using IOCs/ Behavioural(deviation from normal routine traffic) including various network flood events and identify the presence of botnets in the network etc. and detect long-lived connections that may be associated with data-exfiltration.
60	The solution must identify the presence of botnets in the network,DNS spoofing attack.
61	The Solution must be capable of conducting protocol analysis to detect applications using unexpected ports, anomalous transfer of data via certain protocols indicative of tunnelling activity, backdoors, and the use of forbidden application protocols.
62	The solution must utilize anomaly detection methods to identify attacks such as self-propagating malware and worms/viruses, lateral movement.
63	The solution should support detection of malware in Encrypted traffic through analytics.
64	The solution should be able to detect Unknown or encrypted malware, insider threats, policy violations.
65	The Proposed solution should detect policy/ pattern violations.
66	Policy/ Pattern Violation detection rules should be modifyble to include Layer 7 details.
67	The solution should provide a statistics based visualization for the better understanding of the policy/ pattern based detection

68	The system should able to provide the aggregated analysis for the policy/ pattern violation and forensic
	Integration
69	Solution shall support NTP server time synchronization.
70	The NDR solution must be able to interoperate with the Data center, Core and Campus network to track endpoints and provide end-to- end visibility and control.
71	The solution must integrate with existing security solutions like Security Information and Event Management (SIEM), Next- generation Firewalls, Router, Switches, NAC, SOAR, Proxy, WAF, mail gateway etc.
72	The solution should integrate with OpenLDAP, Microsoft Active Directory, RADIUS and DHCP to provide user Identity information in addition to IP address information throughout the system.
73	The system should have a mechanism to consume external lists of known bad IP"s and generate alerts on the same if connection is seen.
74	The NDR system should be able to integrate with external threat feeds.
75	System should do event forwarding for SMTP, SYSLOG & SNMP for high risk issues.
76	The solution should have native integration with CERT CMTX & NCIIPC Threat Feeds
	Reporting
77	Solution should have built-in various reports and can create custom reports like Executive report, detection life cycle report and Health reports etc.
78	The solution should have the ability to generate reports in different formats, such as html, excel, csv and pdf. Reports should be available in real time on demand and should automatically be generated on a scheduled basis. Should support scheduled reports to be delivered via email automatically.
79	Solution should come with predefined & customisable reports and should have ability to run certain reports based on security role.
	Management
80	The proposed solution should have Centralized Management systems supporting role-based administration.
81	The solution must be deployed in Centralized mode with central management and reporting from the single dashboard for the entire deployment.
82	Enables administrators to centrally configure.
83	The solution should have an automated scanner to identify assets and should also be able to schedule the scans
84	The solution should allow taking logs from proxy for the enrichment of the flows.
85	The solution should offer country level traffic visibility and should have dedicated Country wise traffic dashboard
86	The solution should have integration with the MITRE ATT&CK matrix
87	NDR device should be capable to support 10Gbps traffic throughput from day one without any hardware upgradation and should have 4 x 1/10G (copper) traffic capture/ monitoring ports and 2 x 1G management ports along with 5Gbps license from day one.Full packet capture needs to be planned with 7 days retention of PCAP files.

11. Data Base Activity Monitoring

S.No.	Features
1	**Supported Database on-premise**
1.1	Database Security solution should have the licensing options to support features such as Database Activity Monitoring, Vulnerability Assessment, and Virtual Patch Monitoring.

1.2	Proposed database secuirty solution should be agent based solution only and not applaince based solution.
1.3	Proposed solution should support below databases on-premises: • Microsoft SQL 11.0 and later version on Windows platforms • Oracle 8.1 and later versions on Windows, Linux, Solaris, AIX & HPUX • PostgreSQL 9.6 and later versions on Linux • MySQL 5.6 and later versions on Linux • MariaDB 10.0 and later versions on Linux • DB2 10.1 and later versions on Windows, Linux, Solaris, AIX & HPUX • MongoDB 4.0 and later versions on Linux • SAP HANA 2.0 SPS 05 and later versions on Linux • Sybase 12.5 and later versions on Windows, Linux, Solaris, AIX & HPUX
2	**Supported OSs**
2.1	Windows Server OS
2.2	AIX
2.3	HPUX
2.4	Solaris
3	**Availability Management**
3.1	The management platform should have the highability ro to be configured in cluster mode.
3.2	Proposed solution design should supports DC-DR
3.3	Solution should provide option to backup and restore the configuration backups.
4	**Functional features**
4.1	Application should support external authentication methods such as AD/LDAP
4.2	Application should support password policy
4.3	Application should support role based authorization model.
4.4	Application should log all activities, including detailed policy change logs.
4.5	The Proposed Solution should support automatic/dynamic updates to the signature database based on global threat intelligence, ensuring complete protection against the latest threats.
4.6	The solution must be able to perform content scanning for regular expression and patterns and should monitor nested queries
4.7	The solution should be capable of auto discovering sensitive/confidential data, like credit card Numbers, Aadhaar or any PII in the database and offers the ability for customization. The solution should be capable of auto discovering sensitive/ confidential data, like Aadhaar or any PII in the database and offers the ability for customization.
4.8	Proposed solution should have the ability to kill sessions for accessing sensitive data/policy violations and keeping all activity in the logs
4.9	The agent should not require a reboot of OS and DB after installation / configuration. Only one agent to be installed, no third-party agents permitted. All agents regardless of deployment mode should be managed from the centralized management console. The solution should not use any 3rd Party software/support for any purpose
4.10	The proposed solution should be agent based solution to deliver maximum visibility on DB activities. E.g. If a rogue user is initiating physical access to the DB server and making the changes to DB instance, appliance based (in-line appliance) does not provide complete visibility on such actions.
4.11	Tool should record all SQL transactions : DML, DDL , DCL and store this activity securely outside the database on the management.
5	**Platform Security**
5.1	Product Resilient to Network Attacks
5.2	Product should not be dependent on default accounts/passwords
6	**Reports**
6.1	Application should offer dedicated dashboards to pin point specific type of alert within dashboards. It should also offer pre-built reports and report customization flexibility.
6.2	Application should allow creation of customer defined reports

6.3	Application should allow creation of ad-hoc reports
6.4	Application should provide report scheduling
6.5	Dynamic Alert Reports, Dynamic VA Result Reports, and Dynamic System Reports
7	**Compliance Requirements**
7.1	Database Security should be abel to create security rules based on established international standards as below:
7.2	General Data Protection Regulation (GDPR)
7.3	PCI-DSS
7.4	Sarbanes Oxley (SOX)
7.5	SAS-70
7.6	Gramm-Leach-Bliley Act (GLBA)
7.7	HIPAA
7.8	Proposed solution should offer data discovery. Example: discovery scans for PII, GDPR data
7.9	Flexible audit and reporting capabilities suitable for PCI DSS, SOX and HIPAA
8	**Infrastructure change / operational requirements**
8.1	After installing the sensor, proposed solution should not demand for system restart on DBMS side.
8.2	Proposed solution should not be dependant on native configurations of the database. E.g. Solution should not require a change in the database binary
8.3	Proposed solution should not demand any changes in the database application (e.g. truning audit or trace on)
9	**Policies**
9.1	Porposed solution should offer granular level of policy customization e.g. Detect and agenerate and incident if there are DB Users who are accessing the database during non-working(Whitelist Application Users)
9.2	Application should come with pre-configured security policies and it should
9.3	Solution should provide the protection against SQL injection attacks, vulnerable code execution etc.
9.4	Application should allow easy translation of actual database acivity into monitoring/audit policy
10	**Alerts**
10.1	System should provide automated alerts when application errors occur (e.g. when DAM sensor is disconnected from main server/DB is not communicating to database security management server)
10.2	Alerts include the following metadata:
	1. Originating IP Address
	2. DB User
	3. OS User
	4. Full SQL Statement
	5. Accessed tables
	6. Application Name
	7. Module Name
	8. Host Name/Terminal name
	9. Command Type
10.3	Alerts can be sent to external applications:
	1. via e-mail
	2. via syslog
	3. via snmp traps
	4. Other (specify)
11	**Database Vulnerability Assessment (where Applicable)**
11.1	Should be able to scan databases for vulnerability Assessment
11.2	Proposed solution should have the ability to discover all databases

11.3	Configuration assessment should be offered with the solution
11.4	Weak password detection (describe how long weak password detection takes and what affects the speed)
11.5	Allow easy translation of findings into monitoring rules
11.6	Configuration lock-down & change tracking of the policies on the solution
11.7	Practicality of reports (state how long is a typical report per database, what types of reports are provided)
11.8	Does the product provide actionable reports (e.g. recommended SQL conmmands to solve issues discovered by the tool)
11.9	Proposed solution should support 6000+ VA tests e.g. weak passwords, missing patches, CSI benchmark, PCI-DSS regulations, vulnerable codes etc.
12	**Features in detail**
12.1	Monitoring of all database activities and protection against insiders with privileged access
12.2	Granular monitoring of database transactions with real-time alerts and prevention of breaches
12.3	Granular monitoring of queries, objects and stored procedures with real-time alerts and prevention of breaches
12.4	Flexible rules that allow enforcement of corporate security policy with no “false positive” alerts
12.5	Virtual patching of newly discovered database vulnerabilities, providing immediate protection with no DBMS downtime.
12.6	Multiple user roles that facilitate separation of duties
12.7	Specify impact on performance of database, netowrk, I/O. If there are specific features that impact performance (e.g. encryption between system components) please specify
12.8	Easily monitor Access to Sensitive Data (e.g. show all access to credit card table)
12.9	The ability to independently monitor and audit all database activity , including administrator's activity and select transactions.
12.10	Tool should record all SQL transactions : DML, DDL , DCL
12.11	The ability to enforce separation of duties on Database Administrators. (Auditing should include monitoring of DBA activity and solutions should prevent DBA manipulation or tampering with logs or recorded activity
12.12	The ability to generate alert on policy violations. Tool shouldn't just record activity, it should provide real time monitoring and rule based alerting. For example a rule that generates an alert every time a DBA performs a select query on credit card table
12.13	The ability to capture and parse all SQL in real time or near real time
12.14	The ability to track approved database changes implemented in SQL through its rule-based monitoring and alerting system.
12.15	The ability to ensure that a service account only accesses a database from a defined source IP and only runs a narrow group of authorized queries
12.16	Monitor and report on data manipulation language (DML) commands.
12.17	Capture and report on data definition language (DDL) commands.
12.18	Capture and report on SELECT statements.
12.19	Report on detailed SQL, including the source of the request, the actual SQL commands, the database user name, when the request was sent and what database objects the command was issued against.
12.20	Create custom reports and organize on a personalized portal view.
12.21	Group objects (sensitive and financial) and activities for use in reporting.
12.22	Report on database access including logins, client IP, server IP and source program information.
12.23	Perform audits on a specific user and review all commands executed.
12.24	Track execution of stored procedures, including who executed a procedure, what procedure name and when, which tables were accessed as a result
12.25	Track and audit administrative commands such as GRANT,
12.26	Track and report all failed logins.
12.27	Change control process – track DDL execution by DBA, database, time, SQL command, client IP, server IP.

12.28	Create specific rules on observed events, sending SMTP alerts when the rules are violated.
12.29	Capture and report on non-administrators executing DDL.
12.30	Build an interactive graphical representation of database access activity.
12.31	Set-up automatic scheduled data export and archiving to long-term storage.
12.32	Monitor local access & encrypted connections (Oracle ASO, SSL, SSH etc.)
12.33	Provide executive summary / dashboard view
12.34	Provide a means for both online and offline security update capability
12.35	Support for virtualized environments (explain how you support an architecture where both database and applications run on the same physical machine)
12.36	When application has pooled connections, the original IP address and user name can should monitored.
12.37	Solution should have the capability to integrate with SIEM solution.
13	**Support**
13.1	Vendor provides remote support through Phone / Helpdesk / Remote Connectivity. Technical support team should be based of India to deliver quick support in case of high severity issue.
13.2	Vendor should be able to provide onsite support (via local partner or directly)
13.3	Vendor should provide bug fixes, technical support periodically
13.4	The solution provider should deliver 24x7 support.
14	**Documentation**
14.1	Vendor should Provide complete product documentation
14.2	Vendor should provide complete installation and configuration manuals

Advance level use cases incorporating AI/ML Algorithms for generation of unknown threat actors. As an indicative input Firewall/UTN, DNS and WAF are considered at the moment. Similar threat models need to be articulated for other OT infrastructure also. Specific ICS/OT based MITRE tagging is strongly recommended.

Functionality	**Use Case**	**Indicative Minimal Attributes required**	**Remarks**
DNS	I. Excessive number of DNS NXDOMAIN responses on internal sub-domains II. Excessive number of DNS SERVFAIL responses on Internal sub-domains III. Excessive number of failed DNS zone-transfers. IV. Possible fast flux domain detected. V. Persistent traffic to rare non-resolvable domain dns responses. VI. Rare dns host resolved. VII. Rare dns server used. VIII. Randomly generated domain detected on dns response.	✓ Severity ✓ Class-Name ✓ Outcome ✓ Category ✓ HostAddress ✓ Category ✓ SourceIP ✓ SourcePort ✓ Service ✓ Datetime ✓ DestinationHost ✓ Transaction ✓ Action ✓ IPAddress ✓ Type_Name ✓ DeviceAddress ✓ Protocol ✓ Query /Rsponse (Q/R) ✓ Domain Requested ✓ Flags (hex Value)	Requisite attributes are available with DNS Debug logs

Functionality	Use Case	Indicative Minimal Attributes required	Remarks
	IX. Beaconing traffic to rare domains over dns The following additional use can be achieved provided the event logs for these activities are being received. X. DNS response conflicts/cache alteration XI. DNS failed access attempts / brute force XII. Root/admin command execution XIII. Privilege escalation XIV. Access trends deviation XV. Open resolver check XVI. TPI linkages for IOCs/phish etc.		
Firewall	I. Abnormal amount of data aggregated from FTP ports – Firewall II. Abnormal amount of data aggregated from SMB ports – Firewall	✓ Applicationprotocol ✓ baseeventid ✓ bytesin ✓ session status ✓ destinationaddress ✓ destinationport	Complete verbosity of the logs required for subject use case development Following types of logs are required: (a) Traffic

Functionality	Use Case	Indicative Minimal Attributes required	Remarks
	III. Abnormal amount of data transmitted from DNS ports – Firewall IV. Abnormal amount of data transmitted from known file transfer ports – Firewall V. Abnormal amount of data transmitted over covert channels – Firewall VI. Abnormal number of connections on LDAP ports – Firewall VII. Abnormal number of connections on SMB or NETBIOS ports – Firewall VIII. Abnormal number of connections on Telnet ports – Firewall IX. Abnormal number of DNS zone transfers – Firewall X. DNS amplification by frequency of packets – Firewall	✓ ipaddress ✓ accountname ✓ transportprotocol ✓ message/signature ✓ destinationhostname ✓ categoryoutcome ✓ eventtime ✓ date/time ✓ action take by firewall ✓ bytes sent ✓ bytes received ✓ URL accessed ✓ Transport-protocol ✓ Statistical log attributes viz sent-delta & receive-delta ✓ Source interface ✓ Destination interface ✓ UTM action ✓ Log type ✓ Log Subtype ✓ Session ID ✓ Source NAT IP ✓ Destination NAT IP	(b) Threat (c) Web-Filtering (d) Antivirus (e) IPS / IDS (f) VPN

Functionality	Use Case	Indicative Minimal Attributes required	Remarks
	XI. Firewall traffic to randomly generated domains – Firewall XII. Possible external host enumeration over system ports – Firewall XIII. Possible external port scan over system ports – Firewall XIV. Possible host enumeration over system ports – Firewall XV. Possible lateral movement over network traffic – Firewall XVI. Possible port scan over system ports – Firewall XVII. Rare application for known protocols on network traffic – Firewall XVIII. Rare port used by applications on network traffic – Firewall		

Functionality	Use Case	Indicative Minimal Attributes required	Remarks
	IX. Traffic to rare domain on DNS ports – Firewall XX. Traffic to rare server on DHCP ports – Firewall XI. Beaconing traffic to malicious IPs/Domains/CnCs over firewall XII. Rare port used by applications on network traffic XIII. Rare application for known protocols on network traffic The following additional use cases can be achieved provided the event logs for these activities are being received. XXIV. HTTPS traffic over non-https port XXV. Firewall access logs anomalies XXVI. Dictionary attack/Brute force attempts		

Functionality	Use Case	Indicative Minimal Attributes required	Remarks
	XXVII. Multiple sources making session request for an account – In a given timeframe from sources like windows, unix and from different countries /geographic locations/IPs (Land-speed Detection) XVIII. One IP and respective session associated with more than one user ids XXIX. Destination Sweeper in mean time – Threshold of IPs to be set. XXX. Fire-walking or Host sweeper XXXI. Excessive inbound/outbound connections from same source.		

Functionality	Use Case	Indicative Minimal Attributes required	Remarks
	XXII. DOS/DDOS – If particular number of packets blocked by Firewall/UTM. XXIII. VPN two or more country login within say 1 hr by same user. XXIV. Privilege escalation observed from the same IP (i.e elevation to root or admin) XXV. Account logins at unusual hours		
WAF	I. Abnormal number of high severity alerts II. Malicious URLs or OWASP based web application attacks. III. Application based CVE vulnerability exploits with continuous signature update mechanism	✓ Category severity - Severity of alert identified ✓ Category behavior - Type of alert identified - DoS/ SQLietc ✓ Deviceaction - Action taken by the device eg: Allowed / Blocked ✓ Destination-process-name - If applicable	

Functionality	Use Case	Indicative Minimal Attributes required	Remarks
	IV. Rare ports used by a process for high severity endpoint alerts Vulnerable Endpoint monitoring V. Infected Endpoint monitoring Virus and Malicious Code Outbreak VI. Detection of a Virus or Malware The following additional use cases can be achieved provided if relevant signatures are logged and forwarded to. VII. Dictionary attack/Brute force attempts VIII. Multiple sources making session request for an account – In a given timeframe from sources like windows, unix and from	,associated processes with the network connection ✓ Destinationport ✓ Signature Description of signature	

Functionality	Use Case	Indicative Minimal Attributes required	Remarks
	different countries / geographic locations/IPs (Land-speed detection). IX. One IP and respective session associated with more than one user ids. X. Destination Sweeper in mean time – Threshold of IPs to be set. XI. Fire-walking or Host sweeper XII. Privilege escalation observed from the same IP (i.e elevation to root or admin) XIII. Account logins at unusual hours		

Windows Event ID(s)

S. No.	Event ID	Description	Remarks
Category: Scheduled tasks			
1)	4697	This event generates when new service was installed in the system.	
2)	106	This event is logged when the user registered the Task Scheduler task.	
3)	4702	This event generates when scheduled task was updated.	
4)	140	This event is logged when the time service has stopped advertising as a time source because the local machine is not an Active Directory Domain Controller.	
5)	4699	A scheduled task was deleted.	
6)	141	The time service has stopped advertising as a time source because there are no providers running.	
7)	201	This event is logged when the task scheduler successfully completed the task.	
8)	4698	A scheduled task was created. The event description contains the user account that created the task in the Subject section. XML details of the scheduled task are also recorded in the event description under the Task Description section and includes the Task Name.	
9)	4699	A scheduled task was deleted. The Subject section of the event description contains the Account Name that deleted the task as well as the Task Name.	
10)	4700	A scheduled task was enabled. See Event ID 4698 for additional details.	
11)	4701	A scheduled task was disabled. See Event ID 4698 for additional details.	
12)	4702	A scheduled task was updated. The user who initiated the update appears in the Subject section of the event description. The details of the task after its modification are listed in the XML in the event description. Compare with previous Event ID 4702 or 4698 entries for this task to determine what changes were made.	
Category: Services			
13)	4688	It documents each program that is executed, who the program ran as and the process that started this process. It is analysed to rule out process injection.	
14)	4697	A service was installed in the system.	
15)	7045	Created when new services are created on the local Windows machine.	
16)	7034	The service terminated unexpectedly.	

17)	7036	The Windows Firewall/Internet Connection Sharing (ICS) service entered the stopped state or, The Print Spooler service entered the running state.	
18)	7040	The start type of the IPSEC services was changed from disabled to auto start.	
Category: Event Log Manipulation			
19)	1102	Whenever Windows Security audit log is cleared, event ID 1102 is logged.	
20)	104	This event is logged when the log file was cleared.	
Category: Authentication			
21)	4776	The domain controller attempted to validate the credentials for an account.	
22)	4771	This event is logged on domain controllers only and only failure instances of this event are logged (Kerberos pre-authentication failed).	
23)	4768	This event is logged on domain controllers only and both success and failure instances of this event are logged (A Kerberos authentication ticket TGT) was requested.	
24)	4769	Windows uses this event ID for both successful and failed service ticket requests (A Kerberos service ticket was requested).	
25)	*4770*	A service ticket was renewed. The account name, service name, employer IP address, and encryption type are recorded.	
26)	4771	Depending on the reason for a failed Kerberos logon, either Event ID 4768 or Event ID 4771 is created. In either case, the result code in the event description provides additional information about the reason for the failure.	
27)	4776	This event ID is recorded for NTLM authentication attempts. The Network Information section of the event description contains additional information about the remote host in the event of a remote logon attempt. The Keywords field indicates whether the authentication attempt succeeded or failed.	
Category: Sessions			
28)	4624	An account was successfully logged on.	
29)	4625	An account failed to log on.	
30)	4634 & 4647	User initiated logoff/An account was logged off.	
31)	4648	A logon was attempted using explicit credentials.	
32)	4672	Special privileges assigned to new logon.	

33)	4648	A logon was attempted using explicit credentials. When a user attempts to use credentials other than the ones used for the current logon session (including bypassing User Account Control [UAC] to open a process with administrator permissions), this event is logged.	
34)	4672	This event ID is recorded when certain privileges associated with elevated or administrator access are granted to a logon. As with all logon events, the event log will be generated by the system being accessed.	
35)	4778	This event is logged when a session is reconnected to a Windows station. This can occur locally when the user context is switched via fast user switching.	
36)	4779	This event is logged when a session is disconnected. This can occur locally when the user context is switched via fast user switching. It can also occur when a session is reconnected over RDP. A full logoff from an RDP session is logged with Event ID 4637 or 4647 as mentioned earlier.	
Category: Account Management			
37)	4720	A user account was created	
38)	4722	A user account was enabled	
39)	4723	A user attempted to change an account's password.	
40)	4724	An attempt was made to reset an accounts password	
41)	4725	A user account was disabled.	
42)	4726	A user account was deleted.	
43)	4727	A security-enabled global group was created.	
44)	4729	A member was removed from a security-enabled global group.	
45)	4730	A security-enabled global group was deleted.	
46)	4731	A security-enabled local group was created.	
47)	4733	A member was removed from a security-enabled local group.	
48)	4734	A security-enabled local group was deleted.	
49)	4735	A security-enabled local group was changed.	
50)	4737	A security-enabled global group was changed.	
51)	4738	A user account was changed.	
52)	4741	A computer account was created.	
53)	4742	A computer account was changed.	
54)	4743	A computer account was deleted.	
55)	4754	A security-enabled universal group was created.	
56)	4755	A security-enabled universal group was changed	
57)	4728 / 4732 / 4756	group membership changes.	

58)	4757	A member was removed from a security-enabled universal group.	
59)	4758	A security-enabled universal group was deleted.	
60)	4798	A user's local group membership was enumerated. Large numbers of these events may be indicative of adversary account enumeration.	
61)	4799	A security-enabled local group membership was enumerated. Large numbers of these events may be indicative of adversary group enumeration.	
Category: Network Shares			
62)	5140	A network share object was accessed.	
63)	5142	A network share object was added.	
64)	5143	A network share object was modified.	
65)	5144	A network share object was deleted.	
66)	5145	Network share object was checked to see whether employer can be granted desired access.	
Category: Registry Key Values related			
67)	4656	A handle to an object was requested. When a process attempts to gain a handle to an audited object, this event is created. The details of the object to which the handle was requested and the handle ID assigned to the handle are listed in the Object section of the event description.	
68)	4657	A registry value was modified. The user account and process responsible for opening the handle are listed in the event description.	
69)	4658	The handle to an object was closed. The user account and process responsible for opening the handle are listed in the event description. To determine the object itself, refer to the preceding Event ID 4656 with the same Handle ID.	
70)	4660	An object was deleted. The user account and process responsible for opening the handle are listed in the event description. To determine the object itself, refer to the preceding Event ID 4656 with the same Handle ID.	
71)	4663	An attempt was made to access an object. This event is logged when a process attempts to interact with an object, rather than just obtain a handle to the object. This can be used to help determine what types of actions may have been taken on an object (for example, read only or modify data). See Event ID 4656 for additional details.	

Note: The SIEM solution must mandatorily capture the above-mentioned Event IDs, in addition to any other relevant Event IDs required for effective security monitoring.

SECTION 6
I. Conditions of Contract

A. General

1. Definitions

1.1 Terms which are defined in the Contract Data are not also defined in the Conditions of Contract but keep their defined meanings. Bold letters are used to identify defined terms.

Bill of Quantities means the priced and completed Bill of Quantities forming part of the Tender.

Compensation events are those defined in Clause 38 hereunder.

The **Completion Date** is the date of completion of the Works as certified by the Employer in accordance with Sub Clause 46.1.

The **Contract** is the contract between the Employer and the Contractor to execute, complete and maintain the Works. It consists of the documents listed in Clause 2.2 below.

The **Contract Data** defines the documents and other information which comprise the Contract.

The **Contractor** is a person or corporate body whose Tender to carry out the Works has been accepted by the Employer.

The **Contractor's Tender** is the completed Tender document submitted by the Contractor to the Employer.

The **Contract price** is the price stated in the Letter of Acceptance and thereafter as adjusted in accordance with the provisions of the Contract.

Days are calendar days; **months** are calendar months.

A **Defect** is any part of the Works not completed in accordance with the Contract.

The **Defects liability period** is the period named in the Contract Data and calculated from the Completion Date.

The **Employer** is the party who will employ the Contractor to carry out the Works.

Equipment is the Contractor's machinery and vehicles brought temporarily to the Site to construct the Works.

The **Initial Contract price** is the Contract Price listed in the Employer's Letter of Acceptance.

The **Intended Completion Date** is the date on which it is intended that the Contractor shall complete the Works. The Intended Completion Date is specified in the Contract Data. The Intended Completion Date may be revised only by the Employer by issuing an extension of time.

Materials are all supplies, including consumables, used by the contractor for incorporation in the Works.

The **Site** is the area defined as such in the Contract Data.

Specification means the Specification of the Works included in the Contract and any modification or addition made or approved by the Employer.

The **Start Date** is given in the Contract Data. It is the date when the Contractor shall commence execution of the works. It does not necessarily coincide with any of the Site Possession Dates.

A **Subcontractor** is a person or corporate body who has a Contract with the Contractor to carry out a part of the work in the Contract which includes work on the Site.

A **Variation** is an instruction given by the Employer which varies the Works.

The **Works** are what the Contract requires the Contractor to construct, install, and turn over to the Employer, as defined in the Contract Data.

a. "Applicable Law" means the laws and any other instruments having the force of law in India, as they may be issued and in force from time to time;

b. "Contract" means the Contract signed by the Parties, to which these General Conditions of Contract (GC) are attached, together with all the documents listed in Clause 1 of such signed Contract;

c. “Effective Date” means the date on which this Contract comes into force and effect pursuant to Clause GC 2.1

d. “Contract Price” means the price to be paid for the performance of the Services, in accordance with Clause 6;

e. "GC" means these General Conditions of Contract;

f. "Government" means the Government of Karnataka;

g. "Local currency" means Indian Rupees;

h. "Member", shall be the authorized representative of the Contractor specified in the SC to act on their behalf in exercising all the

Contractor's rights and obligations towards the Employer under this Contract.

i. "Party" means the Employer or the Contractor, as the case may be, and Parties means both of them;

j. "Personnel" means persons hired by the Contractor as employees and assigned to the performance of the Services or any part thereof; and 'key personnel' means the personnel referred to in Clause GC4.2 (a)

k. "SC" means the Special Conditions of Contract by which these General Conditions of Contract may be amended or supplemented;

l. "Services" means the work to be performed by the Contractor pursuant to this Contract as described in Appendix A; and

2. Law governing contract

2.1 The law governing the Contract is the Laws of India supplanted by the Karnataka Local Acts.

3. Employer's decisions

3.1 Except where otherwise specifically stated, the Employer will decide contractual matters between the Employer and the Contractor.

4. Delegation

4.1 The Employer may delegate any of his duties and responsibilities to other people after notifying the Contractor and may cancel any delegation after notifying the Contractor.

5. Communications

5.1 Communications between parties which are referred to in the conditions are effective only when in writing. A notice shall be effective only when it is delivered (in terms of Indian Contract Act).

6. Personnel

6.1 The Contractor shall employ the technical personnel (of number and qualifications) as may be stipulated by GOK from time to time during the execution of the work. The technical staff so employed shall be available at site as may be stipulated by the Employer.

6.2 If the Employer asks the Contractor to remove a person who is a member of the Contractor's staff or his work force stating the reasons, the Contractor shall ensure that the person leaves the Site within seven days and has no further connection with the work in the Contract.

7. Employer's and Contractor's risks

7.1 The Employer carries the risks which this Contract states are Employer's risks, and the Contractor carries the risks which this Contract states are Contractor's risks.

8. Employer's risks

8.1 The Employer is responsible for the excepted risks which are:

(a) rebellion, riot commotion or disorder unless solely restricted to employees of the Contractor or his Sub-Contractors arising from the conduct of the Works; or

(b) a cause due solely to the design of the Works, other than the Contractor's design; or

(c) any operation of the forces of nature (in so far as it occurs on the Site) which an experienced contractor:

(i) could not have reasonably foreseen; or

(ii) could reasonably have foreseen, but against which he could not reasonably have taken at least one of the following measures;

(A) prevent loss or damage to physical property from occurring by taking appropriate measures or

(B) insure against such loss or damage

9. Contractor's risks

9.1 All risks of loss of or damage to physical property and of personal injury and death which arise during and in consequence of the performance of the Contract other than the excepted risks are the responsibility of the Contractor.

10. Insurance:

10.1 The Contractor shall prior to commencing the works, effect and thereafter maintain insurances, in the joint names of the Employer and the Contractor, (cover from the first working day after the Start Date to the end of Defects Liability Period), in the amounts stated in the Contract Data:

(a) for loss of or damage to the Works, Plants and Materials and the Contractor's equipment;

(b) for liability of both Parties for loss, damage, death and injury to third parties or their property arising out of the Contractor's performance of the Contract including the Contractor's liability for damage to the Employer's property other than the Works and

(c) for liability of both Parties and of any Employer's representative for death and injury to the Contractor's personnel except to the extent that liability arises from the negligence of the Employer, any Employer's representative or their Employees.

10.2 Policies and certificates for insurance shall be delivered by the Contractor to the Employer for his approval before the Start Date. All such insurance shall provide for compensation to be payable to rectify the loss or damage incurred. All payments received from insurers relating to loss or damage shall be held jointly by the Parties and used for the repair of the loss or damage or as compensation for loss or damage that is not to be repaired.

10.3 If the Contractor fails to effect or keep in force any of the insurances referred to in the previous sub-clauses or fails to provide satisfactory evidence, policies or receipts, the Employer may without prejudice to any other right or remedy, effect insurance for the cover relevant to such default and pay the premiums due and recover the same as a deduction from any other monies due to the Contractor. If no payments is due, the payment of the premiums shall be a debt due.

10.4 Alterations to the terms of an insurance shall not be made without the approval of the Employer.

10.5 Both Parties shall comply with any conditions of the insurance policies.

11. Queries about the Contract Data

11.1 The Employer will clarify queries on the Contract Data.

12. Contractor to construct the Works

12.1 The Contractor shall construct the Works in accordance with the Specification and Drawings.

13. The Works to be completed by the Intended Completion Date

13.1 The Contractor may commence execution of the Works on the Start Date and shall carry out the Works in accordance with the program submitted by the Contractor, as updated with the approval of the Employer, and complete them by the Intended Completion Date.

14. Approval by the Employer:

14.1 The Contractor shall submit Specification and drawings showing the proposed Temporary Works to the Employer, who is to approve them if they comply with the Specifications and Drawings.

14.2 The Contractor shall be responsible for the design of Temporary Works

14.3 The Employer's approval shall not alter the Contractor's responsibility for design of the Temporary Works.

14.4 The Contractor shall obtain approval of third parties to the design of third parties to the design of the temporary Works where required.

14.5 All Drawings prepared by the Contractor for the execution of the temporary or permanent Works, are subject to prior approval by the Employer before their use.

15. Safety

15.1 The Contractor shall be responsible for the safety of all activities on the Site.

16. Discoveries

16.1 Anything of historical or other interest or of significant value unexpectedly discovered on the Site is the property of the Employer. The Contractor is to notify the Employer of such discoveries and carry out the Employer's instructions for dealing with them.

17. Possession of the Site

17.1 The Employer shall give possession of all parts of the Site to the Contractor. If possession of a part is not given by the date stated in the Contract Data the

Employer is deemed to have delayed the start of the relevant activities and this will be Compensation Event.

18. Access to the Site

18.1 The Contractor shall allow the Employer and any person authorized by the Employer access to the Site, to any place where work in connection with the Contract is being carried out or is intended to be carried out and to any place where materials or plant are being manufactured / fabricated / assembled for the works.

19. Instructions

19.1 The Contractor shall carry out all instructions of the Employer which comply with the applicable laws where the Site is located.

20. Procedure for resolution of Disputes:

20.1 If the Contractor is not satisfied with the decision taken by the Employer, the dispute shall be referred by either party to Arbitration within 30 days of the notification of the Employer's decision.

20.2 If neither party refers the dispute to Arbitration within the above 30 days, the Employer's decision will be final and binding.

20.3 The Arbitration shall be conducted in accordance with the arbitration procedure stated in the Special Conditions of Contract.

B. Time Control

21. Program

21.1 Within the time stated in the Contract Data the Contractor shall submit to the Employer for approval a Program showing the general methods, arrangements, order, and timing for all the activities in the Works.

21.2 The Employer's approval of the Program shall not alter the Contractor's obligations. The Contractor may revise the Program and submit it to the Employer again at any time. A revised Program is to show the effect of Variations and Compensation Events.

22. Extension of the Intended Completion Date

22.1 The Employer shall extend the Intended Completion Date if a Compensation Event occurs or a Variation is issued which makes it impossible for Completion to be achieved by the Intended Completion Date.

22.2 The Employer shall decide whether and by how much to extend the Intended Completion Date within 21 days of the Contractor asking the Employer for a decision upon the effect of a Compensation Event or Variation and submitting full supporting information.

23. Delays ordered by the Employer

23.1 The Employer may instruct the Contractor to delay the start or progress of any activity within the Works.

24. Management meetings

24.1 The Employer may require the Contractor to attend a management meeting. The business of a management meeting shall be to review the progress achieved and the plans for remaining work.

24.2 The responsibility of the parties for actions to be taken is to be decided by the Employer either at the management meeting or after the management meeting and stated in writing to be distributed to all who attended the meeting.

C. Quality Control

25. Identifying defects

25.1 The Employer shall check the Contractor's work and notify the Contractor of any Defects that are found. Such checking shall not affect the Contractor's responsibilities. The Employer may instruct the Contractor to search for a Defect and to uncover and test any work that the Employer considers may have a Defect.

26. Tests

26.1 If the Employer instructs the Contractor to carry out a test not specified in the Specification to check whether any work has a Defect and the test shows that it does, the Contractor shall pay for the test and any samples. If there is no Defect the test shall be a Compensation Event.

27. Correction of defects

27.1 The Employer shall give notice to the Contractor of any Defects before the end of the Defects Liability Period, which begins at Completion and is defined in the Contract Data. The Defects Liability Period shall be extended for as long as Defects remain to be corrected.

27.2 Every time notice of a Defect is given, the Contractor shall correct the notified Defect within the length of time specified by the Employer's notice.

28. Uncorrected defects

28.1 If the Contractor has not corrected a Defect within the time specified in the Employer's notice, the Employer will assess the cost of having the Defect corrected, and the Contractor will pay this amount.

D. Cost Control

29.Bill of Quantities (BOQ)

29.1 The BOQ shall contain items for the implantation of Cyber Security Operation Centre, installation, testing, and commissioning work to be done by the Contractor. Please refer BOQ in Section 7 of this tender document.

30. Variations

30.1 The Employer shall have power to order the Contractor to do any or all of the following as considered necessary or advisable during the progress of the work by him

(a) Increase or decrease of any item of work included in the Bill of Quantities (BOQ);
(b) Omit any item of work;
(c) Change the character or quality or kind of any item of work;
(d) Change the levels, lines, positions and dimensions of any part of the work;
(e) Execute additional items of work of any kind necessary for the completion of the works; and
(f) Change in any specified sequence, methods or timing of construction of any part of the work.

30.2 The Contractor shall be bound to carry out the work in accordance with any instructions in this connection, which may be given to him in writing by the Employer and such alteration shall not vitiate or invalidate the contract.

30.3 Variations shall not be made by the Contractor without an order in writing by the Employer, provided that no order in writing shall be required for increase or decrease in the quantity of an item appearing in the BOQ so long as the work executed conforms to the approved drawings.

30.4 The Contractor shall promptly request in writing the Employer to confirm verbal orders and if no such confirmation is received within 15 days of request, it shall be deemed to be an order in writing by the Employer.

31. Payments for Variations

31.1 Payment for increase in the quantities of an item in the BOQ up to 25% of that provided in the Bill of Quantities shall be made at the rates quoted by the Contractor.

31.2 For quantities in excess of 125% of the tendered quantity of an item as given in the BOQ, the Contractor shall be paid at the rate entered in or derived from in the Schedule of Rates (applicable for the area of the work and current at the time of award of contract) plus or minus the overall percentage of the original tendered rates over the current Schedule of Rates prevalent at the time of award of contract.

31.3 If there is no rate for the additional, substituted or altered item of the work in the BOQ, efforts would be made to derive the rates from those given in the BOQ or the Schedule of Rates (applicable for the area of the work and current at the time of award of contract) and if found feasible the payment would be made at the derived rate for the item plus or minus the overall percentage of the original tendered rates over the current Schedule of Rates prevalent at the time of award of contract

31.4 If the Contractor's quotation is determined unreasonable, the Employer may order the Variation and make a change to the Contract Price which shall be

based on Employer's own forecast of the effects of the Variation on the Contractor's costs.

31.5 If the Employer decides that the urgency of varying the work would prevent a quotation being given and considered without delaying the work, no quotation shall be given and the Variation shall be treated as a Compensation Event.

31.6 Under no circumstances the Contractor shall suspend the work on the plea of non-settlement of rates for items falling under this Clause.

32. Submission of bills for payment:

32.1 The Contractor shall submit to the Employer bills as per payment terms and conditions.

32.2 The Employer shall check the Contractor's bill and determine the value of the work executed which shall comprise of (i) value of the quantities of the items in the BOQ completed and (ii) valuation of Variations and Compensation Events

.

32.3 The Employer may exclude any item paid in a previous bill or reduce the proportion of any item previously paid in the light of later information.

33. Payments

33.1 Payments shall be adjusted for deductions for payments, other recoveries in terms of the contract and taxes, at source, as applicable under the law. The Employer shall pay the Contractor within 60 days of submission of bill.

33.2 Items of the Works for which no rate or price has been entered in will not be paid for by the Employer and shall be deemed covered by other rates and prices in the Contract.

II. GENERAL CONDITIONS OF CONTRACT

1. GENERAL PROVISIONS

1.1 Definitions

Unless the context otherwise requires, the following terms whenever used in this Contract have the following meanings:

a. "Applicable Law" means the laws and any other instruments having the force of law in India, as they may be issued and in force from time to time;

b. "Contract" means the Contract signed by the Parties, to which these General Conditions of Contract (GC) are attached, together with all the documents listed in Clause 1 of such signed Contract;

c. "Effective Date" means the date on which this Contract comes into force and effect pursuant to Clause GC 2.1

d. "Contract Price" means the price to be paid for the performance of the Services, in accordance with Clause 6;

e. "GC" means these General Conditions of Contract;

f. "Government" means the Government of Karnataka;

g. "Local currency" means Indian Rupees;

h. "Member", shall be the authorized representative of the Contractor specified in the SC to act on their behalf in exercising all the Contractor's rights and obligations towards the Employer under this Contract.

i. "Party" means the Employer or the Contractor, as the case may be, and Parties means both of them;

j. "Personnel" means persons hired by the Contractor as employees and assigned to the performance of the Services or any part thereof; and 'key personnel' means the personnel referred to in Clause GC4.2 (a)

k. "SC" means the Special Conditions of Contract by which these General Conditions of Contract may be amended or supplemented;

l. "Services" means the work to be performed by the Contractor pursuant to this Contract as described in Appendix A;

1.2 **Law Governing the Contract**

This Contract, its meaning and interpretation, and the relation between the Parties shall be governed by the Applicable Law.

1.3 **Language**

This Contract has been executed in English language, which shall be the binding and controlling language for all matters relating to the meaning or interpretation of this Contract.

1.4 **Notices**

Any notice, request or consent made pursuant to this Contract shall be in writing and shall be deemed to have been made when delivered in person to an authorized representative of the Party to whom the communication is addressed, or when sent by registered mail, telex, e-mail, fax or facsimile to such Party at the address specified in the SC.

1.5 **Location**

The Services shall be performed at such locations as are specified in Appendix A and, where the location of a particular task is not so specified, at such locations, whether in Karnataka or elsewhere, as the Employer may approve.

1.6 **Authorized Representatives**

Any action required or permitted to be taken, and any document required or permitted to be executed, under this Contract by the Employer or the Contractor may be taken or executed by the officials specified in the SC.

1.7 **Taxes and Duties**

The Contractor shall pay such taxes, duties, fees and other impositions as may be levied under the Applicable Law, the amount of which is deemed to have been included in the Contract Price.

2. **Commencement, Completion, Modification and termination of Contract**

2.1 **Effectiveness of Contract**

This Contract shall come into effect on the date the Contract is signed by both Parties or such other later date as may be stated in the SC.

2.2 **Commencement of Services**

The Contractor shall begin carrying out the Services immediately after the date the Contract becomes effective, or at such other date as may be specified in the SC.

2.3 **Expiration of Contract**

Unless terminated earlier pursuant to Clause 2.7, this Contract shall terminate at the end of such time period after the Effective Date as is specified in the SC.

2.4 **Modification**

Modification of the terms and conditions of this Contract, including any modification of the scope of the Services or of the Contract Price, may only be made by written agreement between the Parties.

2.5 **Force Majeure**

2.5.1 **Definition**

For the purposes of this Contract, "Force Majeure" means an event which is beyond the reasonable control of a Party, and which makes a Party's performance of its obligations under the Contract impossible or so impractical as to be considered impossible under the circumstances.

2.5.2 **No Breach of Contract**

The failure of a Party to fulfill any of its obligations under the contract shall not be considered to be a breach of, or default under this Contract insofar as such inability arises from an event of Force Majeure, provided that the Party affected by such an event (a) has taken all reasonable precautions, due care and reasonable alternative measures in order to carry out the terms and conditions of this Contract, and (b) has informed the other Party as soon as possible about the occurrence of such an event.

2.5.3 **Extension of Time**

Any period within which a Party shall, pursuant to this Contract, complete any action or task, shall be extended for a period equal to the time during which such Party was unable to perform such action as a result of Force Majeure.

2.5.4 **Payments**

During the period of their inability to perform the Services as a result of an event of Force Majeure, the Contractor shall be entitled to continue to be paid under the terms of this Contract, as well as to be reimbursed for additional costs reasonably and necessarily incurred by them during such period for the purposes of the Services and in reactivating the Service after the end of such period.

2.6 **Suspension:**

The Employer may by written notice of suspension to the Contractor, suspend all payments to the Contractor hereunder if the Contractor fail to perform any of their obligations under this contract, including the carrying out of the Services, provided that such notice of suspension (i) shall specify the nature of the failure, and (ii) shall request the Contractor to remedy such failure within a period not exceeding thirty (30) days after receipt by the Contractor of such notice of suspension.

2.7 Termination

2.7.1 **By the Employer**

The Employer may terminate this Contract, by not less than thirty (30) days' written notice of termination to the Contractor, to be given after the occurrence of any of the events specified in paragraphs (a) through (e) of this Clause 2.7.1 and sixty (60) days' in the case of the event referred to in (f):

(a) if the Contractor do not remedy a failure in the performance of their obligations under the Contract, within thirty (30) days of receipt after being notified or within such further period as the Employer may have subsequently approved in writing;

(b) if the Contractor (or any of their Members) become insolvent or bankrupt;

(c) if, as the result of Force Majeure, the Contractor are unable to perform a material portion of the Services for a period of not less than sixty (60) days; or

(d) if the Contractor, in the judgment of the Employer has engaged in corrupt or fraudulent practices in competing for or in executing the Contract.

(e) In the event of any security breach, data compromise, violation of confidentiality, or non-compliance with applicable cybersecurity policies, guidelines, or statutory requirements attributable to the firm or its representatives, the Employer shall have the right to terminate the contract immediately, without any notice or financial liability which may leads to blacklisting/debarment of the firm.

For the purpose of this clause:

"corrupt practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of a public official in the selection process or in contract execution.

"fraudulent practice" means a misrepresentation of facts in order to influence a selection process or the execution of a contract to

the detriment of GOK, and includes collusive practice among Contractor (prior to or after submission of proposals) designed to establish prices at artificial non-competitive levels and to deprive GOK of the benefits of free and open competition.

(e) Any events listed in SC.

(f) if the Employer, in its sole discretion and for any reason whatsoever, decides to terminate this Contract.

2.7.2 **By the Contractor**

The Contractor may terminate this Contract, by not less than thirty (30) days written notice to the Employer, such notice to be given after the occurrence of any of the events specified in paragraphs (a) through (c) of this Clause 2.7.2:

(a) if the Employer fails to pay any money due to the Contractor pursuant to this Contract and not subject to dispute pursuant to Clause 7 hereof within forty-five (45) days after receiving written notice from the Contractor that such payment is overdue;

(b) If the Employer is in material breach of its obligations pursuant to this Contract and has not remedied the same with in forty-five (45) days (or such longer period as the Contractor may have subsequently approved in writing) following the receipt by the Employer of the Contractor' notice specifying such breach;

(c) if, as the result of Force Majeure, the Contractor are unable to perform a material portion of the Services for a period of not less than sixty (60) days.

2.7.3 **Cessation of Rights and Obligations**

Upon termination of this Contract pursuant to Clause GC 2.7 , or upon expiration of this Contract pursuant to Clause GC 2.3, all rights and obligations of the Parties hereunder shall cease, except :

(i) such rights and obligations as may have accrued on the date of termination or expiration;

(ii) the obligation of confidentiality set forth in Clause GC 3.3

hereof; (iii)

any right which a Party may have under the Applicable Law.

2.7.4 **Cessation of Services**

Upon termination of this Contract by notice of either Party to the other pursuant to Clauses GC 2.7.1 or GC 2.7.2 hereof, the

Contractor shall, immediately upon dispatch or receipt of such notice, take all necessary steps to bring the Services to a close in a prompt and orderly manner and shall make every reasonable effort to keep expenditures for this purpose to a minimum. With respect to documents prepared by the Contractor and equipment and materials furnished by the Employer, the Contractor shall proceed as provided, respectively, by Clauses GC 3.7 and GC 3.8.

2.7.5 **Payment upon Termination**

Upon termination of this Contract pursuant to Clauses 2.7.1 or 2.7.2, the Employer shall make the following payments to the Contractor:

(a) Payments pursuant to Clause 6 for Services satisfactorily performed prior to the effective date of termination;

(b) except in the case of termination pursuant to paragraphs (a) and (b) of Clause 2.7.1, reimbursement of any reasonable cost incident to the prompt and orderly termination of the Contract.

3. Obligations of the Contractor:

3.1 General

The Contractor shall perform the Services and carry out their obligations hereunder with all due diligence, efficiency and economy, in accordance with generally accepted professional techniques and practices, and shall observe sound management practices, and employ appropriate advanced technology and safe methods. The Contractor shall always act, in respect of any matter relating to this Contract or to the Services, as faithful advisers to the Employer, and shall at all times support and safeguard the Employer's legitimate interests in any dealings with Sub- Contractor or third parties.

3.2 Conflict of Interests

3.2.1 **Contractor Not to Benefit from Commissions, Discounts, etc.**

The payment to the Contractor pursuant to Clause 6 shall constitute the Contractor's sole remuneration in connection with this Contract or the Services, and the Contractor shall not accept for their own benefit any trade commission, discount or similar payment in connection with activities pursuant to this Contract or to the Services or in the discharge of their obligations under the Contract, and the Contractor shall use their best efforts to ensure that the Personnel, any Sub-Contractor, and agents of either of them, similarly shall not receive any such additional remuneration.

3.2.2 **Procurement Rules of Funding Agencies**

If the Contractor, as part of the Services, have the responsibility of advising the Employer on the procurement of goods, works or services, the Contractor shall comply with any applicable procurement guidelines of the funding agencies and shall at all times exercise such responsibility in the best interest of the Employer. Any discounts or commissions obtained by the Contractor in the exercise of such procurement responsibility shall be for the account of the Employer.

3.2.3 **Contractor and Affiliates Not to engage in certain Activities**

The Contractor agree that, during the term of this Contract and after its termination, the Contractor and their affiliates, shall be disqualified from providing goods, works or services (other than the Services and any continuation thereof) for any project resulting from or closely related to the Services.

3.2.4 **Prohibition of Conflicting Activities**

Neither the Contractor nor their Sub-Contractor nor the Personnel shall engage, either directly or indirectly, in any of the following activities:

(a) during the term of this Contract, any business or professional activities in the Government's country which would conflict with the activities assigned to them under this Contract; or
(b) after the termination of this Contract, such other activities as may be specified in the SC.

3.3 **Confidentiality**

The Contractor, their Sub-Contractor, and the Personnel of either of them shall not, disclose any proprietary or confidential information relating to the Project, the Services, this Contract, or the Employer's business or operations without the prior written consent of the Employer. A Non-Disclosure agreement as per prevailing data sharing policy of BESCOM shall be executed between the Employer and Contractor (all the personnel engaged in the activity) before signing of contract and any information is shared.

3.4 **Insurance to Be Taken by the Contractor**

The Contractor (a) shall take and maintain, and shall cause any Sub-Contractor to take and maintain, at their (or the Sub-Contractor', as the case may be) own cost but on terms and conditions approved by the Employer, insurance against the risks, and for the coverage, as shall be specified in the SC; and (b) at the Employer's request, shall provide evidence to the Employer showing that such insurance has been taken and maintained and that the current premiums have been paid for the the entire duration of contract period.

3.5 **Contractor's Actions Requiring Employer's Prior Approval**

The Contractor shall obtain the Employer's prior approval in writing before taking any of the following actions:

(a) entering into a subcontract for the performance of any part of the Services, it being understood (i) that the selection of the Sub-Contractor and the terms and conditions of the subcontract shall have been approved in writing by the Employer prior to the execution of the subcontract, and (ii) that the Contractor shall remain fully liable for the performance of the Services by the Sub-Contractor and its Personnel pursuant to this Contract;

(b) appointing such members of the Personnel not listed by name in Appendix C ("Key Personnel"), and

(c) any other action that may be specified in the SC.

3.6 **Reporting Obligations**

The Contractor shall submit to the Employer the reports and documents specified in Appendix B in the form, in the numbers, and within the periods set forth in the said Appendix.

3.7 **Documents Prepared by the Contractor to Be the Property of the Employer**

All plans, drawings, specifications, designs, reports and other documents and software submitted by the Contractor in accordance with Clause 3.6 shall become and remain the property of the Employer, and the Contractor shall, not later than upon termination or expiration of this Contract, deliver all such documents and software to the Employer, together with a detailed inventory thereof.

3.8 **Equipment and Materials Furnished by the Employer**

Equipment and materials made available to the Contractor by the Employer or purchased by the Contractor with funds provided by the Employer shall be the property of the Employer and shall be marked accordingly. Upon termination or expiration of this Contract, the Contractor shall make available to the Employer an inventory of such equipment and materials and shall dispose of such equipment and materials in accordance with the Employer's instructions. While in possession of such equipment and materials, the Contractor, unless otherwise instructed by the Employer in writing, shall insure them at the expense of the Employer in an amount equal to their replacement value.

4. **Contractor's Personnel and Sub-Contractor**

4.1 **Description of Personnel**

The titles, agreed job descriptions, minimum qualifications and estimated

periods of engagement in the carrying out of the Services of the Contractor' Key Personnel are described in Appendix C.

4.2 **Removal and/or Replacement of Personnel**

(a) Except as the Employer may otherwise agree, no changes shall be made in the Key Personnel. If, for any reason beyond the reasonable control of the Contractor, it becomes necessary to replace any of the Key Personnel, the Contractor shall forthwith provide as a replacement a person of equivalent or better qualifications.

(b) If the Employer finds that any of the Personnel have (i) committed serious misconduct or has been charged with having committed a criminal action, or (ii) have reasonable cause to be dissatisfied with the performance of any of the Personnel, then the Contractor shall, at the Employer's written request specifying the grounds there for, forthwith provide as a replacement a person with qualifications and experience acceptable to the Employer with negative financial implication of 2.50 % of the quoted monthly emoluments against the original key professional at the time of agreement.

(c) The Contractor shall have no claim for additional costs arising out of or incidental to any removal and/or replacement of Personnel.

5. **Obligations of the Employer**

5.1 **Assistance and Exemptions**

Unless otherwise specified in the SC, the Employer shall use its best efforts to ensure that the employer shall:

(a) issue to officials, agents and representatives of the employer all such instructions as may be necessary or appropriate for the prompt and effective implementation of the Services;

(b) assist the Contractor and the Personnel employed by the Contractor for the Services from any requirement to register or obtain any permit to practice their profession or to establish themselves either individually or as a corporate entity according to the Applicable Law;

(c) provide to the Contractor, Personnel any such other assistance as may be specified in the SC.

5.2 **Services and Facilities**

The Employer shall make available to the Contractor and the Personnel, for the purposes of the services and free of any charge, the services, facilities and property described in Appendix D at the times and in the manner specified in said Appendix D, provided that if such services, facilities and property shall not be made available to the Contractor as and when so specified, the Parties shall agree on (i) any time extension that it may be appropriate to grant to the Contractor for the performance of the Services, (ii) the manner in which the Contractor shall procure any such services,

facilities and property from other sources, and (iii) the additional payments, if any, to be made to the Contractor as a result thereof.

6. Payment to the Contractor:

6.1 Contract Price

The Contract price is set forth in the SC. The Contractor's total remuneration shall not exceed the Contract Price and shall be a fixed lump sum including all staff costs, printing, communications, travel, accommodation, and the like, and all other costs incurred by the Contractor in carrying out the Services described in Appendix A.

6.2 Terms and Conditions of Payment

Payments will be made to the account of the Contractor and according to the payment schedule stated in the SC. Unless otherwise stated in the SC, the first payment shall be made against the provision by the Contractor of a bank guarantee for the same amount, and shall be valid for the period stated in the SC. Any other payment shall be made after the conditions listed in the SC for such payment have been met, and the Contractor have submitted an invoice to the Employer specifying the amount due.

7. Settlement of Disputes

7.1 Amicable Settlement

The Parties shall use their best efforts to settle amicably all disputes arising out of or in connection with this Contract or its interpretation.

7.2 Dispute Settlement

Any dispute between the Parties as to matters arising pursuant to this Contract that cannot be settled amicably within thirty (30) days after receipt by one Party of the other Party's request for such amicable settlement may be submitted by either Party for settlement in accordance with the provisions specified in the SC.

8. Debarment/Blacklisting:

Unless otherwise specified in the forgoing clauses, the employer reserve the rights to Debar/Blacklist the tenderer/supplier against specific products, for a period of not less than 3 years as per the guidelines issued by the Government of Karnataka under section 26(A)(B)(C) vide notification No NO:FD 884 Exp-12/2019, Bangalore Dated 7th May 2020, apart from cancellation of the Purchase order, forfeiture of EMD/Security Deposit, towards the lapses/defaults being reported/ found/ observed/ committed as detailed under:

8.1 Debarment/Blacklisting of the firm for a product

b) Non submission of Security deposit within the stipulated/extended time, leading to cancellation of LOI/ Purchase order.

c) Withdrawal of bid or non-execution of supplies within the stipulated/extended period.
d) Supply of spurious/inferior/substandard/Mis-branded/unsafe/refurbished product.
e) Violation and convictions if any under the laws/rules corresponding to supply/execution of product/work similar to tender product/work during the currency of contract period.
f) Non-adherence to Delivery schedules and agreed terms and conditions of the tender, including non-submission of the Performance Security leading the cancellation of the supply order.
g) Any other Corrupt/Fraudulent/unethical business practices

8.2 Debarment/Blacklisting of the firm as a whole

a) Submission of false/misleading/fabricated/invalid/void documents against the bid.
b) In case of a firm debarred/blacklisted by the employer for similar work within a period of one year either under the different Tenders/Purchase orders for any of the reasons stated above or committing similar offence in more than 3 instances, the employer reserves the right to Blacklist the firm as a whole for a period of not less than 3 years as per the provisions of the KTPP Act/Rules and guidelines issued by the Government of Karnataka under section 26(A)(B)(C) vide notification No NO:FD 884 Exp-12/2019, Bangalore Dated 7th May 2020, apart from cancellation of the Purchase order, forfeiture of EMD/Security Deposit
c) Any other Corrupt/Fraudulent/unethical business practices

8.3 The blacklisting of particular product or company/firm will be done without prejudice to other penalties which may be imposed as per the conditions of Tender documents and also to other actions which may be initiated under relevant Acts or any other law of Land. Employer will display names of such blacklisted product(s) and company/firm on its website and also circulate the same among other state Government / Central Government and its procurement agencies.

8.4 The process of Debarment/Blacklisting and Resolution of Disputes:

The process of Debarment/blacklisting by employer will be carried in accordance with the provisions of the KTPP Act/Rules and guidelines issued by the Government of Karnataka under section 26(A)(B)(C) vide notification No NO:FD 884 Exp-12/2019, Bangalore Dated 7th May 2020 In case of a dispute or difference arising between the employer and the supplier relating to any matter arising out of or connected with the Debarment/Blacklisting, such dispute or difference shall be settled as per the provisions of the said Act/Rules and notifications.

9. Exit Management:

9.1. During the contract period (during 5 years) – If the tenderer wishes to take exit from the contract, 6 months' prior notice to be given to the employer. The successful tenderer shall carry out the following activities to complete exit formalities:

9.1.1. Functional & Technical knowledge transfer of all the modules of the CSOC application to the personnel identified by BESCOM.

9.1.1.1. Execute all the documents that may be necessary to effectively transfer the ownership and title, including OEM warranties inrespect of all equipment's/software etc.

a. All related documentation and other configurable items etc., if any,in his possession.
b. List of all IT assets, passwords etc., at all locations to BESCOM.

9.1.1.2. In the event of termination or expiry of the Contract, both the successful tenderer and BESCOM shall comply with the provision of Exit plan.

9.1.1.3. During the exit management period, the successful tenderer uses its best efforts to continue delivery of all regular services. In addition, the successful tenderer shall ensure that complete handover of the processes, products, software licenses, source codes, reports, documents, manuals, data, web content and other intellectual property rights to BESCOM.

9.2. During the contract period (during 5 years)– If the employer wishes to withdraw the contract, 3 months of prior notice will be given to the successful tenderer. the successful tenderer shall will carry out following activities to complete exit formalities:

9.2.1. Functional & Technical knowledge transfer of all the modules of the CSOC to the personnel identified by BESCOM.

9.2.2. Execute all the documents that may be necessary to effectively transfer the ownership and title, including OEM warranties in respect of all equipment's/software etc.,

9.2.3. All related documentation and other configurable items etc., if any,in his possession.

9.2.4. List of all IT assets, passwords etc., at all locations to BESCOM.

9.2.5. In the event of termination or expiry of the Contract, both the successful tenderer and BESCOM shall comply with the provision of Exit plan.

9.2.6. During the exit management period, the successful tenderer uses its best efforts to continue delivery of all regular services. In addition, the successful tenderer shall ensure that complete handover of the processes, products, software licenses, source codes, reports, documents, manuals, data, web content and other intellectual property rights to BESCOM.

9.3. After the contract period (after 5 years) the successful tenderer shall will carry out following activities to complete exit formalities:

9.3.1. Functional & Technical knowledge transfer of all the modules of the application to the personnel identified by BESCOM.

9.3.2. Execute all the documents that may be necessary to effectively transfer

the ownership and title, including OEM warranties in respect of all equipment's/software etc.,

9.3.3. All related documentation and other configurable items etc., if any, in his possession.

9.3.4. List of all IT assets, passwords etc., at all locations to BESCOM.

9.3.5. In the event of termination or expiry of the Contract, both the successful tenderer and BESCOM shall comply with the provision of Exit plan.

9.3.6. During the exit management period, the successful tenderer uses its best efforts to continue delivery of all regular services. In addition, the successful tenderer shall ensure that complete handover of the processes, products, software licenses, source codes, reports, documents, manuals, data, web content and other intellectual property rights to BESCOM.

9.3.7. The Performance Bank Guarantee furnished by the Successful Tenderer shall remain valid until completion of exit management and shall be released only upon written certification by BESCOM confirming satisfactory completion thereof. In case of any breach, non-performance, partial performance, or failure in exit management obligations, BESCOM shall have the right to invoke the Performance Bank Guarantee to the extent of the value of the assets, services, or obligations not transferred or not supported, without prejudice to BESCOM's right to claim damages or seek any other remedy under law.

10. Tax Deducted at Source (TDS)

10.1. Deduction of TDS: Tax shall be deducted at source (TDS) from payments made to the successful tenderer, as applicable, in accordance with the provisions of the Income Tax Act, 1961, as amended from time to time, and rules made thereunder.

10.2. Applicable Rates: TDS shall be deducted at the rates prescribed under the relevant sections of the Income Tax Act, 1961, or at such rates as notified by the Government of India from time to time.

10.3. PAN Requirement: The tenderer shall mandatorily furnish a valid Permanent Account Number (PAN). In the absence of PAN or in case of invalid PAN, TDS shall be deducted at higher rates as per Section 206AA of the Income Tax Act, 1961.

10.4. Statutory Compliance: The Employer shall deposit the deducted TDS amount with the appropriate tax authority within the stipulated time and shall issue the TDS certificate (Form 16A) to the tenderer as per statutory requirements.

10.5. No Liability on Employer: Any tax liability, including interest, penalty, or surcharge arising out of incorrect declaration or non-compliance by the

tenderer shall be the sole responsibility of the tenderer. The Employer shall not be liable for the same.

10.6. No Grossing Up: Prices quoted by the tenderer shall be inclusive of all taxes and duties, except GST. No claim for grossing up of contract value on account of TDS deduction shall be entertained.

10.7. Statutory Changes: Any change in applicable tax laws or TDS rates during the contract period shall be governed by prevailing statutory provisions, and deductions shall be made accordingly.

10.8. **GST Registration Details:** The tenderer shall furnish valid GSTIN, place of supply details, and other statutory information required for GST-TDS compliance. Any incorrect or invalid GST details shall be the responsibility of the tenderer.

10.9. Deposit and Certificate: The Employer shall deposit the deducted GST-TDS amount with the appropriate tax authority within the stipulated time and shall issue the GST-TDS Certificate (Form GSTR-7A) to the tenderer as prescribed under GST law.

10.10. Adjustment in GST Returns: The tenderer shall be responsible for claiming credit of GST-TDS in their GST returns. Any mismatch, non-credit, or compliance issue shall not be attributable to the Employer.

III. SPECIAL CONDITIONS OF CONTRACT

GCC Clause No./SCC Clause No.	Amendments of, and Supplements to, Clauses in the General Conditions of Contract
G.C 1.1(h)	The Member in Charge is NOT APPLICABLE.
G.C 1.4.1	The addresses are: Employer: Office of the General Manager (Ele), DAS, SG & TIC, BESCOM Integrated Control Centre-1, 2nd Sector, 24th Main, 17th Cross, Opp. BWSSB, HSR Layout, Bangalore-560102 E-mail: gmdas@bescom.co.in
G.C 1.4.2	Notice shall be deemed to be effective as follows: (a) In the case of personal delivery or registered post, on delivery; (b) In the case of Fax/e-mail, 24 hours following confirmed transmission.
G.C 1.6	The General Manager (Ele), DAS, SG & TIC, BESCOM is the authorized Representative of BANGALORE ELECTRICITY SUPPLY COMPANY LIMITED (BESCOM) (here after called as EMPLOYER). The Employer's authorized Representative shall take all the actions required with respect to the execution of this Contract. However, Employer Authorized Representative can recommend to the Employer regarding termination of contract with relevant contractual documents. Contractor shall nominate his authorized representative for execution of this contract through appropriate Power of Attorney supported by Board Resolution The authorized representatives for employer: The General Manager (Ele), DAS, SG & TIC, BESCOM
G.C 1.7.1	The service is inclusive of GST and applicable taxes and The Contractor shall pay the taxes, duties, fees, levies and other impositions levied under the existing, amended or enacted laws during life of this contract and the Employer shall perform such duties in regard to the deduction of such tax as may be lawfully imposed.
G.C 2.1	The date on which this Contract shall come into effect is: *Date of issue of Detailed Work Award (DWA)*
G.C 2.2	The Contractor shall begin carrying out the Services immediately after the date the Contract becomes effective.
G.C 2.3	This contract shall be valid for a period of 5 years and six months from the date of issue of DWA
G.C 2.7.1	(e) **Performance of Contractor:** i. Contractor is expected to fully adhere to all the provisions of detailed scope of work and shall be fully responsible for successful implementation of the Project in accordance with the provisions of the works contract agreement and other schedules agreed between the Employer /Employer's Representative and the works contractors. Any failure of Contractor in notifying to the Employer and work contractor on non-compliance of the work contract agreement and other schedules by the work contractor, non-adherence to the provisions of detailed scope of work and non-adherence to the time schedule prescribed under detailed scope of work amounts to nonperformance of the Contractor. In such a condition, Employer has the right to encash the performance security and terminates the contract.

	ii. If the Contractor fails to deploy the key and sub key manpower as agreed in the detailed scope of work, will amount to non-performance of contractor. In such a condition, Employer has the right to encash the performance security and terminates the contract. iii. During the execution of works; if the Contractor fails to perform their obligations as specified in detailed scope of work either with respect to progress monitoring and or quality control by the Contractor team the same shall be treated as non-performance of contract.
G.C 3.4	The risks and the coverages shall be: (1) Third Party motor vehicle liability insurance as required under Motor VehiclesAct,1988, in respect of motor vehicles operated in India by the Contractor or their Personnel or any Sub-Contractor or their Personnel, for the period of Consultancy; (2) Third Party liability insurance for the period of Contract; (3) Employer's liability and workers' compensation insurance in respect of the Personnel of the Contractor and of any Sub-Contractor, in accordance with the relevant provisions of the Applicable Law, as well as, with respect to such Personnel, any such life, health, accident, travel or other insurance as may be appropriate; (4) Professional liability insurance, with a minimum coverage equal to total contract value for this contract; and (5) Insurance against loss of or damage to (i) equipment purchased in whole or in part with funds provided under this Contract, (ii) the Contractor' property used in the performance of the Services, and (iii) any documents prepared by the Contractor in the performance of the Services.
G.C 3.7	The Contractor shall not use these documents for purposes unrelated to this Contract without the prior written approval of the Employer.
G.C 6.2	The amount of Contract is the approved cost of the service inclusive of applicable GST.
G.C 6.2	The Contractor shall submit the bill in approved proforma (one original and three copies) in accordance with the Contract Agreement and agreed billing schedule in Work award to the successful tenderer enclosing necessary supporting documents. The documents to be submitted will be mutually agreed between selected Tenderer and BESCOM during Contract signing. • Except as otherwise specifically provided in the Contract, the Contractor shall bear and pay all taxes, duties and levies assessed on the Contractor, its Sub-contractors or their employees by all municipal, state or national government authorities in connection with the Project. The prices quoted by the Contractor shall be inclusive of all taxes, duties and levies. The taxes, duties and levies (including abatement/taxable composition, if any) as applicable will be paid to the Contractor against documentary evidence. • Payment will be made as per conditions in the letter of Award to the successful tenderer. • The Employer shall verify the bill and supporting documents after receipt of bill from the Contractor. The Employer shall release the payment after deducting applicable taxes, penalties/liquidated damages and other recoverable. All the payments made by the Employer will be in Indian Rupee only. No payment made by the Employer

	herein shall be deemed to constitute acceptance by the Employer of the goods or services or any part(s) thereof. • If any excess payment has been made by the Employer due to difference in quoted price in the proposal and Contractor's invoice, the Employer may without prejudice to its rights recover such amounts by other means after notifying the Contractor or deduct such excess payment from any payment subsequently falling due to the Contractor. • At its own discretion, the Employer shall make payments either through crossed bank cheque or electronic bank transfer. • Wherever applicable, tax deduction certificates shall be issued at the end of the month against deduction of statutory taxes • Payment will be arranged by Assistant General Manager (F&C), DAS, BESCOM upon submission of invoices by the contractor duly certified by Manager(TIC), Assistant General Manager (ISD) and Deputy General Manager (TIC) and Counter Signed by General Manager (DAS, SG & TIC). • BESCOM reserves the right to forfeit the Performance Bank Guarantee and terminate the contract if the contractor fails to commence the first time & second time assessment activity on the date intimated by BESCOM. • The total penalty shall not exceed 10% of the contract value.
G.C 7	**LAW, JURISDICTION, DISPUTES RESOLUTION AND ARBITRATION** a) Party claiming that a Dispute has arisen under this Agreement must give the other Party a written notice of the particulars of the Dispute. b) Any dispute(s) or difference(s) arising out of or in connection with the Contract shall, to the extent possible, be settled amicably between the Parties. c) If the party fails to resolve such a dispute or difference by mutual consultation within thirty (30) days from the commencement of such dispute and difference, either party may require that the dispute be referred to arbitration under the Arbitration and Conciliation Act, 1996 (Indian) and subsequent Amendments made thereon, to be adjudicated by a sole arbitrator to be appointed by mutual agreement of both the parties and the award of the arbitrator shall be final and conclusive and binding upon both the Parties. (The date of commencement of the dispute shall be taken from the date when this clause reference is quoted by either party in a formal communication clearly mentioning existence of dispute or as mutually agreed). d) The place of arbitration shall be in Bangalore. The arbitral procedure shall be conducted in English language. e) The cost of arbitration including the fees of arbitrator shall be borne by both the parties equally. f) During the settlement of disputes and Arbitration proceedings, both parties shall be obliged to carry out their respective obligations under the contract. g) The award of the arbitrator shall be final and conclusive and binding upon the parties. h) The courts of Bangalore only shall have the exclusive jurisdiction to deal with any issues arising out of this agreement.
S.C 1.	**Performance Security:** 1.1 The Contractor shall provide guarantee for the performance of the contract within 15 days after the receipt of the Letter of intent to award. The Performance security shall be in the form of an unconditional Bank guarantee issued by a scheduled bank located in India amounting to **5% of the Contract value or as per KTPP requirement** and in the format prescribed or in such other format as may be agreed between the employer and the contractor. The cost and complying with the requirement of this clause shall be borne by the contractor. No interest will be payable on the Performance security.

	1.2 The Performance Bank Guarantee shall be valid until the contractor has executed and completed the works therein in accordance with the Contract at least for a period of 90 days after the project completion. 1.3 Claims Under Performance Guarantee Prior to including a claim under the performance Guarantee the Employer shall in every case notify the contractor stating the nature of the default in respect of which the claim is made
S.C 2	**Liquidated Damages:** ▪ The Contractor should bear in mind that time is the essence of the Contract. If the Contractor fails to complete the Scope of Work of the Project or any part thereof within the Time for Completion or any extension thereof as per clause 2.5.3 of GC, the Employer shall recover from the Contractor as Liquidated Damage (LD) for such default and not as a penalty, without prejudice to the Employer's Other remedies under the Contract. For imposition of LD, the loss/ damages suffered by the Employer due to delays by the Contractor are the basic criteria. ▪ The recovery towards compensation should take place when loss/damage has actually taken place on account of delay caused by the Contractor. Even if there is a delay in execution of the Contract and reasons for delay are attributable to the Contractor but the Employer has not suffered any actual out-of-pocket loss specifically due to delay in performance of the Contract, as evidenced by written documentation setting forth the basis for such loss, no sum as LD is recoverable from the Contractor. However, in such cases, a nominal LD as described in this clause will be recovered. ▪ Calculation of Liquidated Damages: A sum equivalent to half percent (0.5%) of the total price in Price Bid for each week of delay or part thereof which will elapse between the schedule time for completion and actual time for completion of the Project. ▪ The total recovery against liquidated damage in all cases, however, shall not exceed ten percent (10%) of the total price in Price Bid. If the amount of LD exceeds this limit, the Employer reserves right to terminate the Contract.
SC.3	**Time period for various activities:** *Refer: Detailed scope of work*
SC.4	Successful tenderer shall coordinate with the project monitoring agency appointed by BESCOM for the project and shall duly incorporate the inputs on time.

All other conditions are applicable as per KTPP Act.

DATA SHEET

Information to Tenderers

No.	Section	Title	Details
1	1.1	Name of Employer	BESCOM or its authorized representative.
2	1.2	**The method of selection is:**	**Quality-and Cost-Based Selection (QCBS) Method.**
3	1.3	Description of Assignment.	As per Detailed Scope of Work.
4	1.4	Financial Bid to be submitted together with Technical Bid	YES
		Name of the assignment is:	Implementation of Cyber - Security Operation Centre (C-SOC) for BESCOM
5	1.5	The Assignment is Phased	No, the Assignment is continuous in nature.
6	1.6.1	A Pre Bid Conference will be held :	Yes.
		Pre bid conference time & date	Time & date as notified in the KPP portal
7	1.6.2	A pre-bid conference venue	As notified in the KPP portal
8	1.7	Employers Inputs	The General Manager, (DAS,SG&TIC) will provide the available information.
9	1.8	The Employer envisages the need for continuity for downstream work	Not Applicable
10	1.9	Clauses on fraudulent and Corrupt practices	Contract will be terminated as per Sub-Clause 2.7.1 of General Conditions of Contract.
11	2.0	Clarification of any item of the Tender Document	Clarifications may be sought from Office of the General Manager, (DAS, SG &TIC), corporate Office, BESCOM, K R Circle, Bengaluru on or before the dead line set for seeking clarifications in the following format only

			<table><tr><th>Sl. no.</th><th>Section no. / Clause no.</th><th>Page no.</th><th>Description/ Reference/ Subject</th><th>Clarification Sought</th></tr><tr><td></td><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td><td></td></tr></table>Email: **gmdas@bescom.co.in** Also, tenderer can submit on line clarification through KPP portal through query option on or before the deadline notified in KPP portal.
12	2.1	Language of the Bid	English
13	2.2	Tenderer participating in RFP may associate with other Tenderers	Tenderer participating in RFP should not associate with other participating Tenderer.
14	2.3	The estimated number of key and sub key professional staff months required for the assignment is:	The estimated number of key and sub key professional staff is indicated in Detailed scope of work.
15	2.4	The minimum qualification and experience required for the proposed key and sub key professional staff is:	As per schedule in Detailed scope of work and scope of Tenderer.
16	2.5	Official Language Language of reports	English
17	2.6	Training is an important feature of this Assignment.	No.
18	2.7	Additional Information in the Technical Bid includes.	NIL
19	2.8	Validity of Bid	180 (One Hundred and Eighty) days from the last date of submission of bid.
20	2.9	Last Date and time for submission of bid	As notified in the Government of Karnataka KPP portal
21	3.0	The address to send information to the Employer is:	As mentioned in KPP portal
22	3.1	The number of points to be given under each	

		of the evaluation criteria :	**Please (Technical evaluation criteria) of PQR** **The minimum technical score required to qualify is : 70 Points (St >= 70)**
23	3.2	Location for Negotiations	At Employers Office
24	3.3	Commencement of Assignment	From the day of issue of Detailed Work Award (DWA).
25	3.4	Performance Security	5% (Five percent) of the Contract value

SECTION 7: Payment Terms and Milestones – C-SOC Implementation

Payments for the C-SOC Implementation Project shall be made on a **milestone basis**, duly linked to the **Bill of Quantities (BoQ)** and subject to satisfactory completion of activities as per the **Scope of Work, Technical Specifications, SLA and GCC/SCC provisions**. Payments shall be made against the invoice raised after duly certifying the invoices by Manager (TIC), AGM(ISD), DGM (SG&TIC) & countersigned by GM(DAS, SG&TIC), BESCOM.

I. Payment for One Time Setup Cost:

Sl. No.	Milestone	BoQ Reference	Scope Covered	Payment (% of Contract Value)	Payment Conditions
1	Supply & Procurement of Hardware	Part-A, Part-B, Part-C	Supply and delivery of all hardware, appliances, servers, storage, HA log collectors, networking equipment, system software and all tools and software as detailed in BoM items	**55%**	On delivery, physical verification and acceptance of all BoM items by BESCOM
2	Installation, Commissioning & SOC Control Room Setup	Part-B, Part-C, Part D (Licensing charges as per BoQ)	Installation, commissioning and basic configuration of DC infrastructure and complete C-SOC Control Room setup	**25%**	On successful installation and readiness certification
3	Factory Acceptance Test (FAT) User Acceptance Test (UAT) Post-Implementation & SLA Compliance	Part-A, Part-B, Part-C	Integration of C-SOC components and successful FAT as per Technical Specifications. Successful UAT, validation of use cases, workflows, dashboards and SOC processes. Successful operation of C-SOC for 6 months from DWA date	**20%**	On submission and approval of FAT reports, UAT sign-off,

Deliverables by the tenderer:

The tenderer shall provide the following reports/documents at the time of submission of invoices respectively against the works or when requested by BESCOM (not limited to the below):

- Invoices
- Tool purchase invoices
- Warranty/guarantee details for hardware

- Software licenses and subscriptions (to be procured in the name of BESCOM)
- MeitY-empanelled certificates
- CERT-In empanelled certificates
- Insurance coverage documents on hardwares and softwares
- SLA documents
- Human resources qualification certificates and certifications.

Note: all the tools/software licenses/hardware's/subscriptions purchased should be in the name of BESCOM.

II. **Payment for Human Resources:** Will be paid on monthly basis after the implementation phase

III. **Payment for subscription:** Will be paid annually.

2. Payment Schedule

Table-1

Sl No	BOQ Sub Heading	Summary of Cost Data Sheet	BOQ Reference	Amount payable
1	**A**	**Tools Subscription Charges**	**A1-A22**	
2	**B**	**C-SOC Room Infrastructure setup**	**B1-B22**	
3	**C**	**Tool Licensing & Maintenance Charges for 5 years**	**C1 to C3**	
4	**D**	**C-SOC Human Resource Cost during Maintenance (24*7) for 5 years**	**D1 to D8**	
5	**Grand Total**			

Table-2

Cyber Security Operation Centre Bill of Quantities				
One Time Set Up Cost				
A	**Tools Set Up Cost**			
1	Next Generation Security Information and Event Management (NG SIEM) with 25000EPS	Lot	1	Considered Licensing for typical 25000 events per second or equivalent per Discom including setup, for Enterprise IT systems, Public Facing Applications (like revenue, billing, CRM, Mobile Apps for consumers etc.), OT systems & DR site integration.
2	Security Orchestration, Automation and Response (SOAR)	Lot	1	As per SIEM licensing
3	Network Behaviour Anomaly Detection (NBAD)	Lot	1	Considered for Licensing of 500Mbps* Network traffic per Discom
4	User and Entity Behaviour Analytics (UEBA)	Lot	1	Profile creation and monitoring capability of typical 6000 Users or equivalent per Discom, has been considered
5	Database Activity Monitoring (DAM)	Lot	1	Licensed for max of 50 Databases or equivalent per Discom including all installation
6	Threat Intelligence Platform (TIP)	Lot	1	
7	Endpoint Detection & Response (EDR)	Lot	1	
8	Vulnerability Management (VM)			
9	Mobile App Security (RASP)	Lot	1	
10	External Attack Surface Management (EASM)	Lot	1	
11	DDoS Protection	Lot	1	
12	WAF + API + Bot Protection	Lot	1	
13	Unified Endpoint Management (UEM)	Lot	1	
14	SSO Integration	Lot	1	
15	Infrastructure/Cloud Log Onboarding	Lot	1	
16	Documentation & Policy Framework	Lot	1	
17	Training & Knowledge Transfer			
17	Application Whitelisting & Secure Web Gateway (SWG)/Secure	Lot	1	
18	Service Edge(SSE)/Proxy Gateway	Lot	1	
19	NDR/NBAD			
20	Air-Gapped IT/OT Secured Communication (IT/OT Appliance)	Lot	1	
22	Integration of Proposed C-SOC with other IT/OT Infrastructure (DC, DR of DISCOM, AMISP, State Data Centre etc.))	Lot	1	

B	C-SOC Room Infra			
1	2x2 55 inch Video Wall with CPU	No	2	for SOC Control Room setup (as per space availability)
2	24x7 Workstation Specifications: CPU (Processor) — Power & Parallelism; AMD Ryzen 9 7950X3D or AMD Ryzen Threadripper PRO 7955WX Motherboard- For AMD Ryzen: X670E / B650E chipset; For Threadripper PRO: WRX80 chipset Storage Primary (OS + Apps): 2 TB NVMe SSD (PCIe 4.0/5.0) Secondary (Workspace / Projects): 4 TB NVMe or SATA SSD Memory (RAM): 64 GB DDR5-6000+ (minimum); 128 GB DDR5 Networking: Dual-band Wi-Fi 6E + Bluetooth 5.3 (optional based on preference); 1 GbE or 2.5 GbE onboard LAN	Nos.	15	for SOC Shift operator and other security analysts
3	Log Collectors in HA (in active-passive mode of operation)	Pair	4	The quantity considered per Discom includes Log Collector per network i.e. OT, DR, Enterprise IT applications(ERP, bespoke intranet applications) , IT Public facing (revenue, billing, CRM, Mobile Apps for consumers etc.) applications. OPLC in HA per network of installation has been considered.
4	Necessary Server & Storage infrastructure / Infrastructure for Virtualized environment, for complete SOC solution (working in HA mode at DC with minimum N-1 redundancy) along with necessary Licensing for Kernel of Virtualization Environment and Server OS platforms and Virtualization software. Server minimum 700 Cores , Storage minimum 300 TB with Backup appliance including software and related systems	Lot	1	Storage sizing should include capability of storing 6 months log on the fly and balance one year log in archived /compressed mode. Hardware sizing to be considered should be capable of running full functionality of the SOC modules on Highavailability in N-1 scenario (i.e.. in One Node failure condition)
5	Firewall on HA (in active-passive mode of operation) with 5 year support & subscription	Pair	1	Firewall may be considered if the SOC infrastructure to be planned for hosting in an independent network infrastructure
6	Server Rack	Nos	2	2 nos. rack considered to have rack level redund
7	Switches & Router	Lot	1	As per integration requirement and network architecture
8	Cable & accessories	Lot	1	
9	Installation, configuration and training	LS	LS	
10	System Software (as per architecture OS/virtualization/RDBMS etc.)	Lot	1	
11	Load Balancers	No	2	
12	Multifunctional Printer	Nos	2	
13	Civil Work (Furniture, Flooring, Ceiling, Interiors, Fire Rated Doors, Glass Doors, Cabling with dual connectivity, Trenches,cable trays and raceways etc.) with AMC for 5 years	LS	1	
14	Electric Work (Earthing, Lighting, Power DB, Cabling with dual connectivity etc.) with AMC for 5 years	LS	1	
15	Access Control Solution (For all doors in CSOC Control Room)	Lot	1	
16	CCTV with NVR Solution (with Cameras to cover entire area of C-SOC Control Room	Lot	1	
17	Intelligent addressable fire detection and alarm system with Smoke Detector & sufficient Fire Extinguishers (HSSD (High Sensitivity Smoke Detection Solution) VESDA (Very Early Smoke Detection Apparatus)	Lot	1	
18	Centralised Air conditioning Solution for C-SOC Command and Control Centre	Lot	1	
19	Rodent Repellent System & Water Leak Detection System	Lot	1	
20	UPS of capacity 20 KVA and battery bank with 30 minutes backup on full load for CSOC Control Room	Lot	2	

Annual Maintainance Cost				
C	**Tool AMC**			
1	SIEM Component Licensing charges per year	Year	5	
1.1	Log Ingestion (~1500 GB/day) , Retention (1 yr hot + cold),Threat Packs / Use Cases,Admin & Support			
	Total			
2	EDR & Vulnerability Management Licensing charges per year			
2.1	EDR Licensing for 6000 nos	Per endpoint/ Year	5	
2.2	Vulnerability Scanning, Threat Intel Add-ons	Year	5	
	Total			
3	Other Technical Component			
3.1	SOAR + TIP Integration,	Year	5	
3.2	WAF / API / DDoS			
3.3	Cloud Security Logging			
3.4	RASP (App Security)			
3.5	UEM & SSO Licenses			
3.6	External Attack Surface Monitoring/ Dark Web Monitoring, Reputation Monitoring(5 Primary Domain, 15 Public Facing Assets, 10 Executive Roles)			
3.7	SIEM and SOAR Integration Only – Existing EDR Endpoints (1303): Integration of existing EDR server with SIEM/SOAR, security event correlation, alerting, and incident analysis. No EDR deployment or licensing applicable.	1303	Per Endpoint / Per Year	
	Total			
D	C-SOC Human Resource			
1	SOC Level 1 Analyst (6 nos)	Year	5	
2	SOC Level 2 Analyst (3 nos)	Year	5	
3	SOC Specialist (1 no)	Year	5	
4	SOC Level 1 Analyst (GRC Team) (1 no)	Year	5	
5	SOC Level 2 Analyst (GRC Team) (1 no)	Year	5	
6	Level 1 Engineer (Endpoint Tools) (1no)	Year	5	
7	Level 2 Engineer (Endpoint Tools) (1no)	Year	5	
8	Level 2 Engineer (Application & Network Security)(1no.)	Year	5	

SECTION 8. APPENDICES

Appendix A: Description of the Services

Refer: Detailed scope of work and special conditions of the contract. (Scope of work)

Appendix B: Deliverables by Contractor and performance of Contractor

Refer: Detailed scope of work. (Scope of work)

Appendix C: Key Personnel

Refer: Detailed scope of work. (Scope of work)

Appendix D: Services and Facilities to be provided by the Employer

Refer: Detailed scope of work (Scope of work)

Appendix E: Breakdown of Contract Price in Indian Rupees

Refer: Financial proposal submission form.

Appendix F: FORM OF PERFORMANCE SECURITY (PERFORMANCE BANK GUARANTEE)

(Clause-2.9 of Information to Contractor)

(To be stamped in accordance with Applicable Stamp Act, if any)

Ref: **.....** Bank Guarantee:**.....**Date: **.....**

To,
The General Manager (DAS, SG & TIC),
BESCOM Integrated Control Centre-1,
2nd Sector, 24th Main, 17th Cross,
Opp. BWSSB, HSR Layout,
Bangalore-560102

WHEREAS**.....**[Name and address of Contractor] hereinafter called "the Contractor") has undertaken, in pursuance of Contract No. **.....** dated ..... to provide the services on terms and conditions set forth in this Contract to "_____**".** Form of Guarantee for performance security deposit (hereinafter called the "the Contract").AND WHEREAS it has been stipulated by you in the said Contract that the Contractor shall furnish you with a Bank Guarantee by a recognized bank for the sum specified therein as security for compliance with his obligations in accordance with the Contract;

AND WHEREAS we have agreed to give the Contractor such a Bank Guarantee;

NOW THEREOF we hereby affirm that we are the Guarantor and responsible to you, on behalf of the Contractor up to a total of ..... [amount of Guarantee] ..... [in words], such sum being payable in the types and proportions of currencies in which the Contract Price is payable, and we undertake to pay you, upon your first written demand and without cavil or argument, any sum or sums within the limits of ..... [amount of Guarantee] as aforesaid without your needing to prove or to show grounds or reasons for your demand for the sum specified therein.

We hereby waive the necessity of your demanding the said debt from the Contractor before presenting us with the demand.

We further agree that no change or addition to or other modification of the terms of the Contract or of the services to be performed there under or of any of the Contract documents which may be made between you and the Contractor shall in any way release us from any liability under this guarantee, and we hereby waive notice of any such change, addition or modification.

The liability of the Bank under this Guarantee shall not be affected by any change in the constitution of the Contractor or of the Bank.

Notwithstanding anything contained herein before, our liability under this guarantee is restricted to Rs..... (Rs .....) and the guarantee shall remain valid till .....Unless a claim or a demand in writing is made upon us on or before..... all our liability under this guarantee shall cease.

This guarantee shall be valid until 90 days from the date of expiry of the Defects Liability Period.

Signature and Seal of the Guarantor..... In presence of
Name and Designation
(Name, Signature &Occupation)

Name of the Bank
Address
(Name & Occupation)

Date.....

Note: This format is for the information of the contractor and is <u>not</u> to be completed and uploaded on the KPP portal.

Appendix G:

EMD Declaration
(To be uploaded on the Tenderer's letter head)

I, hereby submit a declaration that the tender submitted by the undersigned, on behalf of the tenderer ..... (Name of the Tenderer), shall not be withdrawn or modified during the period of validity or extended period of validity.

I, on behalf of the tenderer..... (Name of the Tenderer), also accept the fact that in case the tender is withdrawn or modified during the period of its validity / extended validity period or if we fail to sign the contract in case the contract is awarded to us or we fail to submit a performance security and Additional performance security, if any, before the deadline fixed in the tender document, then ..... (Name of the tenderer) will be debarred for participation in the tendering process for the procurements of this procurement entity for a period of one year from the date of default.

Signature of the Authorised signatory
Office seal

Appendix H:

PROFORMA OF EXTENSION OF BANK GUARANTEE
(To be uploaded on the Tenderer's letter head)

Ref …… Date …….

TO

The General Manager (DAS, SG & TIC),
BESCOM Integrated Control Centre-1,
2nd Sector, 24th Main, 17th Cross,
Opp. BWSSB, HSR Layout,
Bangalore-560102

Dear Sir,

Sub: Extension of Bank Guarantee No ……for Rs……favouring yourselves, expiring on …… on account of M/s……in respect of Contract No ……dated…….(hereinafter called original Bank Guarantee).

At the request of M/ s ……,We……Bank, Branch Office at ……and having its Head Office at ……do hereby extend our liability under the above mentioned Guarantee No …… Dated …… for a further period of ……Years/Months from ……to expire on ……Except as provided above, all other Terms and Conditions of the original Bank Guarantee No ……dated ……shall remain unaltered and binding.

Please treat this as an integral part of the Original Bank Guarantee to which it would be attached.

Yours faithfully,

For ……
Manager/Agent/Accountant
Power of Attorney No ……
Dated ……

SEAL OF BANK

NOTE: The non-judicial stamp paper of appropriate values shall be purchased in the name of the bank who has issued the Bank Guarantee.

Appendix I:

PROFORMA OF LETTER OF UNDERTAKING

(To be executed on Non-Judicial paper of requisite value)

Ref ……. Date …….

TO

Dear Sir,

1. I*/We* have read and examined the following Bid Documents relating to the……(full scope of Work).

   b. Notice Inviting Tender.
   c. Conditions of Contract containing Sections: 'Invitation to Bid, 'Instructions to Tenderer", "General Terms & Conditions of Contract (GCC)"
   d. Special Conditions of Contract (SCC) along with Annexure …… to …….
   e. Technical Specifications.

2. I / We hereby submit our Bid and undertake to keep our Bid Valid for a period of One Hundred and Eighty days (180 days) from the last date of submission of bid.

3. I/We hereby further undertake that during said period I/We shall not vary/alter or revoke my/our Bid.

This undertaking is in consideration of BESCOM agreeing to open my/our Bid and consider and evaluate the same for the purpose of Award of Work in terms of provisions of Clause entitled "Award of Contract" Section ITB, Conditions of Contract in the Bid Documents.

Should this Bid be accepted, I*/We* also agree to abide by and fulfil all the terms, conditions of provision of the above mentioned Bid Documents.

Witness:

Signature
Date:
Name & Address
Name …….
Designation …….
Name of Co ……. (in Block Letters)
*Strike out whichever is not applicable.

Signature along with Seal of Co.
…….
(Duly authorized to sign the Tender On behalf of the Contractor)

Appendix J:
(To be uploaded on the Tenderer's letter head)

Tenderer's Name & Address:

To,
The General Manager (DAS, SG & TIC),
BESCOM Integrated Control Centre-1,
2nd Sector, 24th Main, 17th Cross,
Opp. BWSSB, HSR Layout,
Bangalore-560102

NO DEVIATION CERTIFICATE

With reference to our Bid Proposal No..... dated ..... for ....., we hereby confirm that we have read the provisions of the Contract, the stipulation of these Clause are acceptable to us, and we have not taken any deviation whatsoever to these Clauses:

a) **Terms of Payment:**
Clause 6.2 of General Conditions of Contract-GCC, Volume-I
b) **Bid Security /EMD:**
Clause 2.4.3 of Section 2 – Instruction to Tenderer-ITB.
c) **Contract Performance Guarantee.**
Clause 2.8 of Section 2 - Instruction to Tenderer-ITB
d) **Penalty for Delay.**
Clause 6.2 of General Conditions of Contract-GCC

We further confirm that any deviation to the above Clauses at SL. No. (a) to (d) found anywhere in our Bid Proposal, implicit or explicit, shall stand unconditionally withdrawn, without any Cost implication whatsoever to

Date: Signature along with Seal of Co.
.....

(Duly authorised to sign the Tender On behalf of the Tenderer)
Name .....
Designation .....
Name of Co ..... (in Block Letters)

Appendix K:

IMPORTANT: TO BE UPLOADED IN KPP PORTAL

PROFORMA OF SELF DECLARATION FOR TENDERER NOT HAVE BEEN DEFAULTED IN SUPPLIES/SERVICES/INSTALLATION AND COMMISSIONING

(Tenderer shall upload notarized Self-Declaration)

Ref …… Date ……

NOT DEFAULTED DECLARATION

To,
The General Manager (DAS, SG & TIC),
BESCOM Integrated Control Centre-1,
2nd Sector, 24th Main, 17th Cross,
Opp. BWSSB, HSR Layout,
Bangalore-560102

Dear Sir,

Sub: Tender Enquiry No. _____to "_____"

We hereby declare that, we have not been defaulted in supplies/services/ installation and commissioning against any of the previous Purchase Orders/Work Awards placed by any ESCOMs/ any electrical distribution utilities/ PSUs/ Govt. utilities as on the date of bid opening.

Date:

Signature along with Seal of Co.
……
(Duly authorised to sign the Tender On behalf of the Tenderer)
Name ……
Designation ……
Name of Co …… (in Block Letters)

Appendix L:

IMPORTANT: TO BE UPLOADED IN KPP PORTAL

PROFORMA OF SELF DECLARATION FOR TENDERER NOT HAVE BEEN BLACK LISTED IN SUPPLIES/SERVICES/INSTALLATION AND COMMISSIONING
(Tenderer shall upload notarized Self-Declaration)

Ref …… Date …….

NOT BLACK LISTED DECLARATION

To,

The General Manager (DAS, SG & TIC),
BESCOM Integrated Control Centre-1,
2nd Sector, 24th Main, 17th Cross,
Opp. BWSSB, HSR Layout,
Bangalore-560102

Sir,
Sub: Tender Enquiry No. _____to "_____"

We hereby declare that, we have not been black listed in supplies/services /installation and commissioning against Purchase orders/Work Awards placed by any ESCOMs / any electrical distribution utilities/ PSUs/ Govt. utilities as on the date of bid opening.

Date:

Signature along with Seal of Co.
…….
(Duly authorised to sign the Tender On behalf of the Tenderer)
Name …….
Designation …….
Name of Co …….. (in Block Letters)

Appendix M:

IMPORTANT: TO BE UPLOADED IN KPP PORTAL

PROFORMA OF SELF DECLARATION FOR BORDER SHARING OR NOT SHARING BY TENDERERS

(Tenderer shall upload notarized Self-Declaration)

Ref …… Date ……

To,
The General Manager (DAS, SG & TIC),
BESCOM Integrated Control Centre-1,
2nd Sector, 24th Main, 17th Cross,
Opp. BWSSB, HSR Layout,
Bangalore-560102

Dear Sirs,
I*/We* have read and examined the requirement of the tender condition stipulated against clause No. 13 of Section IFB of Bid Documents relating to the Tender Enquiry No. …… for …… (full scope of Work).

I*/We* hereby undertake to declare that (Applicable in case of Tenderers from Countries not sharing Border with India)

I*/We* have read the clause regarding restrictions on procurement from a Tenderer of a country which shares a land border with India;
I*/We* certify that ……(Tenderer) is not from such a country which shares a land border with India. I hereby certify that our bid fulfils all requirements in this regard and is eligible to be considered.

OR

I*/We* hereby undertake to declare that (Applicable in case of Tenderers from Countries sharing Border with India)

I*/We* have read the clause regarding restrictions on procurement from a Tenderer of a country which shares a land border with India;
I*/We* certify that ……(Tenderer) is from such a country which shares a land border with India and has been registered with the Competent Authority. I hereby certify that our bid fulfils all requirements in this regard and is eligible to be considered and also evidence of valid registration issued by the Competent Authority is uploaded.

This undertaking is in consideration of BESCOM agreeing to open my/our Bid and consider and evaluate the same for the purpose of issue of purchase order in terms of provisions of clause entitled "Issue of Purchase Order" Section ITB, conditions of contract in the bid documents.

Date: Signature along with Seal of Co.

……
(Duly authorised to sign the Tender On behalf of the Tenderer)
Name ……
Designation ……
Name of Co …… (in Block Letters)

***Strike out whichever is not applicable.**
Please Note: Among the above two declarations, only one which is applicable is to be declared